ESET Smart Security 4

Guida dell’utente

Microsoft® Windows® 7 / Vista / XP / 2000 / 2003 / 2008



we protect your digital worlds

ESET Smart Security 4

Supporto tecnico globale: www.eset.eu/support
Supporto tecnico America del nord: www.eset.com/support

REV.20091023-007

Sommario

1. ESET Smart Security 4 4
1.1 Novità 4
1.2 Requisiti di sistema 5

2. Installazione 6
2.1 Installazione tipica 6
2.2 Installazione personalizzata 7
2.3 Utilizzo delle impostazioni originali 9
2.4 Inserimento di nome utente e password 9
2.5 Controllo computer su richiesta 9

3. Guida introduttiva 10
3.1 Introduzione all'interfaccia utente: modalità 10
3.1.1 Verifica del funzionamento del sistema 10
3.1.2 Cosa fare se il programma non funziona correttamente 10
3.2 Configurazione dell'aggiornamento 11
3.3 Impostazione area attendibile 11
3.4 Impostazione del server proxy 12
3.5 Configurazione protezione 12

4. Utilizzo di ESET Smart Security 13
4.1 Protezione antivirus e antispyware 13
4.1.1 Protezione del file system in tempo reale 13
4.1.1.1 Impostazione del controllo 13
4.1.1.1.1 Oggetti da controllare 13
4.1.1.1.2 Scansione (scansione quando si verifica un evento) 13
4.1.1.1.3 Parametri ThreatSense aggiuntivi per i file appena creati e modificati 13
4.1.1.1.4 Configurazione avanzata 13
4.1.1.2 Livelli di pulitura 13
4.1.1.3 Quando modificare la configurazione della protezione in tempo reale 14
4.1.1.4 Controllo della protezione in tempo reale 14
4.1.1.5 Cosa fare se la protezione in tempo reale non funziona 14
4.1.2 Protezione client e-mail 14
4.1.2.1 Controllo POP3 14
4.1.2.1.1 Compatibilità 15
4.1.2.2 Integrazione con client e-mail 15
4.1.2.2.1 Aggiunta di notifiche al corpo di un messaggio e-mail 15
4.1.2.3 Eliminazione delle infiltrazioni 15
4.1.3 Protezione accesso Web 16
4.1.3.1 HTTP, HTTPS 16
4.1.3.1.1 Gestione degli indirizzi 16
4.1.3.1.2 Browser 16
4.1.4 Controllo del computer 17
4.1.4.1 Tipo di controllo 17
4.1.4.1.1 Controllo standard 17
4.1.4.1.2 Controllo personalizzato 17
4.1.4.2 Oggetti da controllare 18

4.1.4.3 Profili di scansione 18
4.1.5 Filtro dei protocolli 18
4.1.5.1 SSL 18
4.1.5.1.1 Certificati attendibili 19
4.1.5.1.2 Certificati esclusi 19
4.1.6 Impostazione parametri motore ThreatSense 19
4.1.6.1 Configurazione degli oggetti 19
4.1.6.2 Opzioni 19
4.1.6.3 Pulizia 20
4.1.6.4 Estensioni 20
4.1.6.5 Limiti 20
4.1.6.6 Altro 21
4.1.7 Rilevamento di un'infiltrazione 21
4.2 Personal firewall 21
4.2.1 Modalità di filtro 21
4.2.2 Blocca tutto il traffico di rete: disconnessione rete 22
4.2.3 Filtraggio disattivato: consenti tutto il traffico 22
4.2.4 Configurazione e uso delle regole 22
4.2.4.1 Creazione di nuove regole 23
4.2.4.2 Modifica delle regole 23
4.2.5 Configurazione aree 23
4.2.6 Stabilire la connessione: rilevamento 23
4.2.7 Registrazione 24
4.3 Protezione antispam 24
4.3.1 Riconoscimento automatico antispam 25
4.3.1.1 Aggiunta di indirizzi a whitelist 25
4.3.1.2 Contrassegnare messaggi come spamming 25
4.4 Aggiornamento del programma 25
4.4.1 Configurazione dell'aggiornamento 25
4.4.1.1 Profili di aggiornamento 26
4.4.1.2 Configurazione avanzata dell'aggiornamento 26
4.4.1.2.1 Modalità di aggiornamento 26
4.4.1.2.2 Server proxy 27
4.4.1.2.3 Connessione alla LAN 27
4.4.1.2.4 Creazione di copie di aggiornamento: Mirror 27
4.4.1.2.4.1 Aggiornamento dal Mirror 28
4.4.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror 29
4.4.2 Come creare le attività di aggiornamento 29
4.5 Pianificazione attività 29
4.5.1 Scopo della pianificazione attività 29
4.5.2 Creazione di nuove attività 29
4.6 Quarantena 30
4.6.1 Mettere i file in quarantena 30
4.6.2 Ripristino dalla quarantena 30
4.6.3 Invio di file dalla cartella Quarantena 30
4.7 File di rapporto 31
4.7.1 Manutenzione rapporto 31
4.8 Interfaccia utente 31
4.8.1 Avvisi e notifiche 32
4.9 ThreatSense.Net 32
4.9.1 File sospetti 33
4.9.2 Statistiche 33
4.9.3 Invio 34
4.10 Amministrazione remota 34
4.11 Licenza 35

5. Utente avanzato 36

5.1 Impostazione del server proxy 36
5.2 Esportazione o importazione di impostazioni 36
5.2.1 Esportazione delle impostazioni 36
5.2.2 Importazione delle impostazioni 36
5.3 Riga di comando 36
5.4 ESET SysInspector 37
5.4.1 Interfaccia utente e utilizzo dell'applicazione 37
5.4.1.1 Comandi del programma 38
5.4.1.2 Navigare in ESET SysInspector 38
5.4.1.3 Confronta rapporti 39
5.4.1.4 SysInspector come componente di ESET Smart Security 4 39
5.5 ESET SysRescue 40
5.5.1 Requisiti minimi 40
5.5.2 Come creare un CD di ripristino 40
5.5.2.1 Cartelle 40
5.5.2.2 ESET Antivirus 40
5.5.2.3 Avanzate 40
5.5.2.4 Supporto USB di avvio 40
5.5.2.5 Masterizzazione 40
5.5.3 Utilizzo di ESET SysRescue 41
5.5.3.1 Utilizzo di ESET SysRescue 41

6. Glossario 42

6.1 Tipi di infiltrazioni 42
6.1.1 Virus 42
6.1.2 Worm 42
6.1.4 Rootkit 42
6.1.5 Adware 42
6.1.6 Spyware 43
6.1.7 Applicazioni potenzialmente pericolose 43
6.1.8 Applicazioni potenzialmente indesiderate 43
6.2 Tipi di attacchi remoti 43
6.2.1 Attacchi DoS (Denial of Service) 43
6.2.2 Poisoning DNS 43
6.2.3 Attacchi worm 43
6.2.4 Scansione porte 43
6.2.5 Desincronizzazione TCP 44
6.2.6 SMB Relay 44
6.2.7 Attacchi ICMP 44
6.3 E-mail 44
6.3.1 Pubblicità 44
6.3.2 Hoax: truffe e bufale 45
6.3.3 Phishing 45
6.3.4 Riconoscimento di messaggi spamming 45
6.3.4.1 Regole 45
6.3.4.2 Filtro Bayes 45
6.3.4.3 Whitelist 45
6.3.4.4 Blacklist 46
6.3.4.5 Controllo lato server 46

1. ESET Smart Security 4

ESET Smart Security 4 è il primo software con un nuovo approccio a una sicurezza realmente integrata. Sfrutta la velocità e la precisione di ESET NOD32 Antivirus e la versione più recente del motore di scansione ThreatSense®, combinate con i moduli-personalizzati Personal firewall e Antispam. Il risultato è un sistema intelligente costantemente allerta contro gli attacchi e il software dannoso che possono compromettere il computer.

ESET Smart Security non è un agglomerato disordinato di vari prodotti riuniti in un unico pacchetto, come le offerte di altri produttori. Si tratta del risultato di sforzi a lungo-termine per combinare la massima protezione con un impatto minimo sul sistema. Le tecnologie avanzate basate sull'intelligenza artificiale sono in grado di eliminare in modo proattivo la penetrazione di virus, spyware, trojan horse, worm, adware, rootkit e altri attacchi trasportati da Internet senza rallentare le prestazioni del sistema o interrompere l'attività del computer.

1.1 Novità

L'esperienza di sviluppo a lungo termine degli esperti ESET è dimostrata dall'architettura completamente nuova del programma ESET Smart Security, che garantisce la massima capacità di rilevamento con requisiti di sistema minimi. Questa soluzione di protezione complessa contiene moduli dotati di molte opzioni avanzate. Nell'elenco che segue è riportata una breve panoramica sui singoli moduli.

- **Antivirus e antispyware**

Questo modulo si basa sul motore di scansione ThreatSense®, utilizzato per la prima volta nel pluripremiato sistema NOD32 Antivirus. Nella nuova architettura di ESET Smart Security, il motore ThreatSense® è stato ottimizzato e migliorato.

Funzione	Descrizione
Pulizia migliorata	Il sistema antivirus ora pulisce ed elimina in modo intelligente la maggior parte delle infiltrazioni rilevate, senza richiedere l'intervento dell'utente.
Modalità di scansione in background	Il controllo del computer può essere eseguito in background, senza rallentare le prestazioni del computer.
File di aggiornamento di minori dimensioni	I processi di ottimizzazione principali consentono di generare file di aggiornamento di dimensioni minori rispetto alla versione 2.7. Inoltre, è stata migliorata la protezione dei file di aggiornamento dagli eventuali danni.
Protezione dei client di posta più diffusi	Ora è possibile effettuare il controllo della posta in arrivo non solo in MS Outlook, ma anche in Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.
Miglioramenti minori	– Accesso diretto ai file system per una maggiore velocità effettiva. – Blocco dell'accesso ai file infetti. – Ottimizzazione per Centro sicurezza PC Windows, incluso Vista.

- **Personal firewall**

Il Personal firewall esegue il controllo di tutto il traffico tra un computer protetto e altri computer della rete. Firewall ESET dispone delle funzioni avanzate elencate di seguito.

Funzione	Descrizione
Scansione delle comunicazioni di rete di livello inferiore	Il controllo delle comunicazioni di rete su Data Link Layer consente a Firewall ESET di bloccare un'ampia gamma di attacchi, che altrimenti non sarebbero rilevabili.
Supporto IPv6	Il Firewall ESET visualizza gli indirizzi IPv6 e consente agli utenti di creare regole per tali indirizzi.
Monitoraggio file eseguibili	Il controllo modifica i file eseguibili per sconfiggere le infezioni. È possibile consentire la modifica dei file delle applicazioni firmate.
Controllo dei file integrato con HTTP(s) e POP3(s)	Controllo dei file integrato nei protocolli di applicazione HTTP(s) e POP3(s). Gli utenti sono sempre protetti durante la navigazione in Internet o quando scaricano le e-mail.
Sistema di rilevamento intrusione	Capacità di riconoscere il carattere della comunicazione di rete e vari tipi di attacchi di rete e un'opzione per impedire automaticamente tale comunicazione.
Supporto modalità interattiva, automatica, riconoscimento, basata su criteri e automatica con eccezioni	Gli utenti hanno la possibilità di selezionare se le azioni del firewall verranno eseguite automaticamente o di impostare le regole in modo interattivo. La comunicazione nella modalità basata su-criteri viene gestita in base a regole predefinite dall'utente o dall'amministratore di rete. La Modalità riconoscimento crea e salva automaticamente le regole, inoltre, è ideale per la configurazione iniziale del firewall.
Sostituisce Windows Firewall integrato	Sostituisce Windows Firewall integrato e interagisce con il Centro sicurezza PC di Windows, pertanto l'utente è sempre informato sullo stato di sicurezza del sistema. Nell'impostazione predefinita, l'installazione di ESET Smart Security disattiva Windows Firewall

- **Antispam**

Il modulo Antispam ESET filtra le e-mail indesiderate e aumenta la sicurezza della comunicazione elettronica.

Funzione	Descrizione
Segnalazione posta in arrivo	A tutta la posta in arrivo viene assegnato un punteggio da 0 (messaggio non spam) a 100 (messaggio spam) e trasferita di conseguenza nella cartella della posta indesiderata o in una cartella personalizzata creata dall'utente. È possibile eseguire il controllo parallelo della posta in arrivo.
Supporto di un'ampia gamma di tecniche di scansione	– Analisi Bayes – Controllo basato su regole – Controllo database delle firme digitali globale
Integrazione completa con client di posta	Protezione antispam disponibile per gli utenti dei client di Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.
Disponibile la modalità di selezione manuale dei messaggi di spam	È presente un'opzione per selezionare/deselezionare manualmente le e-mail come spam.

- **Altre**

Funzione	Descrizione
ESET SysRescue	ESET SysRescue consente all'utente di creare un CD/DVD/USB di avvio contenente ESET Smart Security, in grado di essere eseguito in modo indipendente dal sistema operativo. Viene utilizzato soprattutto per ripulire il sistema dalle infiltrazioni più ostinate.
ESET SysInspector	L'applicazione ESET SysInspector ispeziona il computer in modo approfondito. Adesso è integrata direttamente in ESET Smart Security. Contattando il nostro servizio di Assistenza clienti dall'opzione Guida e supporto tecnico > Richiesta di supporto all'Assistenza clienti (consigliato), è possibile scegliere di includere un rapporto di ESET SysInspector sullo stato del proprio computer.
Protezione documenti	La funzione Protezione documenti serve a eseguire la scansione dei documenti di Microsoft Office prima della loro apertura e i file scaricati automaticamente da Internet Explorer, come gli elementi di Microsoft ActiveX.
Autodifesa	La nuova tecnologia Autodifesa protegge i componenti di ESET Smart Security dai tentativi di disattivazione.
Interfaccia utente	L'interfaccia utente adesso è in grado di lavorare in modalità non grafica, consentendo il controllo dalla tastiera di ESET Smart Security. La maggiore compatibilità con le applicazioni di lettura dello schermo consente ai non vedenti di controllare il programma con maggiore efficienza.

1.2 Requisiti di sistema

Per il corretto funzionamento di ESET Smart Security e ESET Smart Security Business Edition, il sistema deve soddisfare i seguenti requisiti hardware e software:

ESET Smart Security:

Windows 2000, XP	400 MHz a 32 bit/64 bit (x86/x64) 128 MB di RAM di memoria di sistema 130 MB di spazio su disco disponibile Super VGA (800 × 600)
Windows 7, Vista	1 GHz a 32 bit/64 bit (x86/x64) 512 MB di RAM di memoria di sistema 130 MB di spazio su disco disponibile Super VGA (800 × 600)

ESET Smart Security Business Edition:

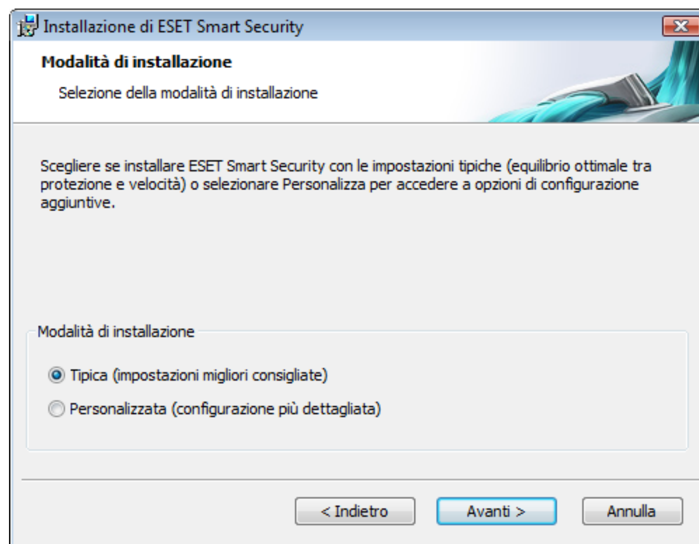
Windows 2000, 2000 Server, XP, 2003 Server	400 MHz a 32 bit/64 bit (x86/x64) 128 MB di RAM di memoria di sistema 130 MB di spazio su disco disponibile Super VGA (800 × 600)
Windows 7, Vista, Windows Server 2008	1 GHz a 32 bit/64 bit (x86/x64) 512 MB di RAM di memoria di sistema 130 MB di spazio su disco disponibile Super VGA (800 × 600)

2. Installazione

Dopo aver effettuato l'acquisto, è possibile scaricare il programma di installazione di ESET Smart Security dal sito Web di ESET. Il programma viene fornito in un pacchetto ess_nt**_***.msi (ESET Smart Security) o essbe_nt**_***.msi (ESET Smart Security Business Edition). Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi della configurazione di base. Esistono due tipi di installazione disponibili con diversi livelli di dettagli di impostazione:

1. Installazione tipica

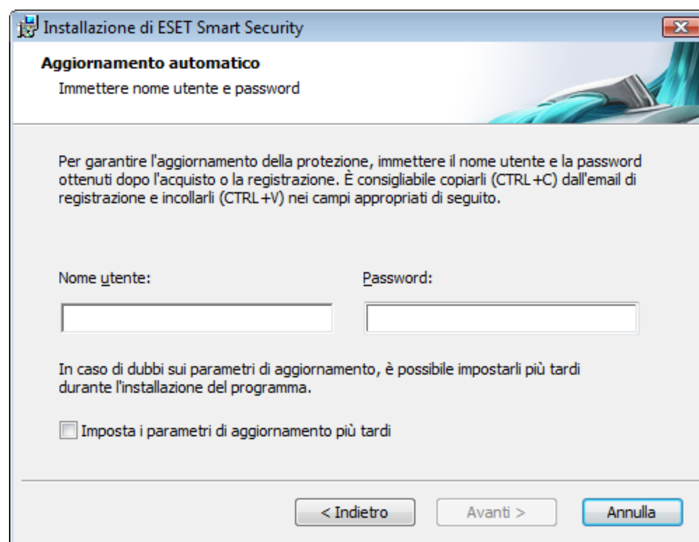
2. Installazione personalizzata



2.1 Installazione tipica

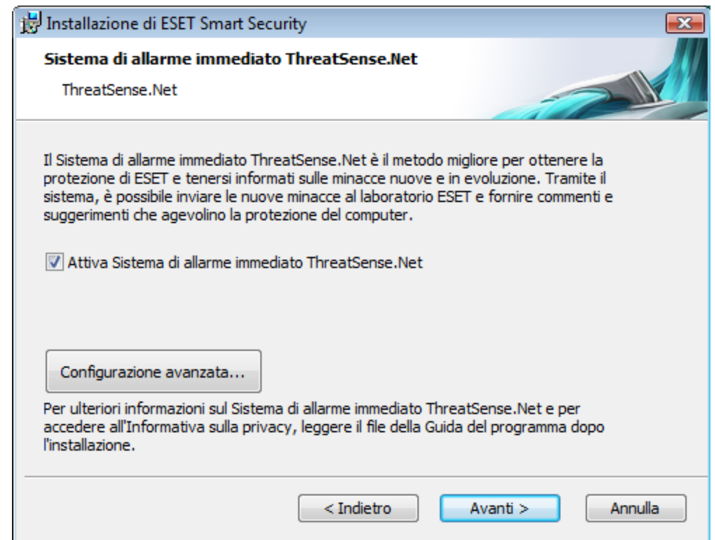
L'installazione tipica è consigliata agli utenti che desiderano installare ESET Smart Security con le impostazioni predefinite. Le impostazioni predefinite del programma offrono il massimo livello di protezione, caratteristica apprezzata soprattutto dagli utenti che non desiderano configurare impostazioni molto dettagliate.

La prima importante operazione da eseguire è l'inserimento di nome utente e password per l'aggiornamento automatico del programma, funzione fondamentale per garantire una protezione costante del sistema.



Immettere nei campi corrispondenti **Nome utente** e **Password**, cioè i dati di autenticazione ottenuti dopo l'acquisto o la registrazione del prodotto. Se non si dispone ancora di nome utente e password, selezionare l'opzione **Imposta i parametri di aggiornamento più tardi**. È possibile inserire i dati di autenticazione anche successivamente, direttamente dal programma.

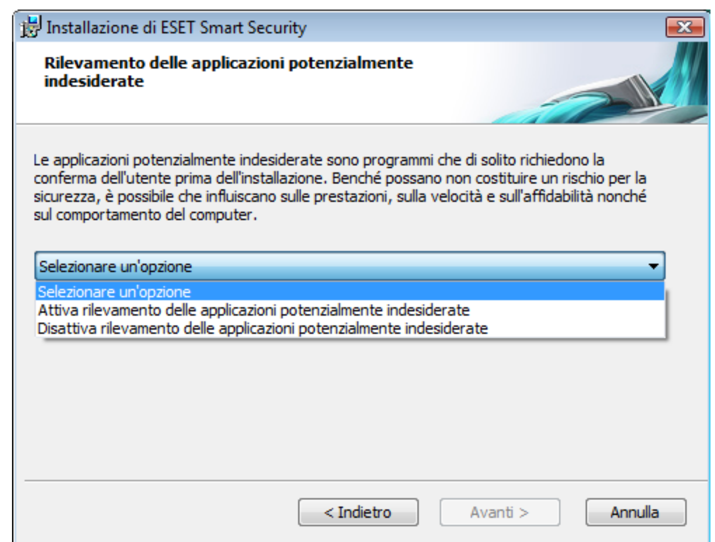
Il passaggio successivo dell'installazione prevede la configurazione del Sistema di allarme immediato (ThreatSense.Net). Il Sistema di allarme immediato (ThreatSense.Net) garantisce che ESET venga informata in modo tempestivo e continuato sulle nuove infiltrazioni, per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuove minacce al laboratorio dei virus ESET, dove verranno analizzate, elaborate e aggiunte al database delle firme antivirali.



Nell'impostazione predefinita, la casella di controllo **Attiva Sistema di allarme immediato ThreatSense.Net** è selezionata in modo da attivare questa funzione. Per modificare le impostazioni dettagliate per l'invio di file sospetti, fare clic su **Configurazione avanzata...**

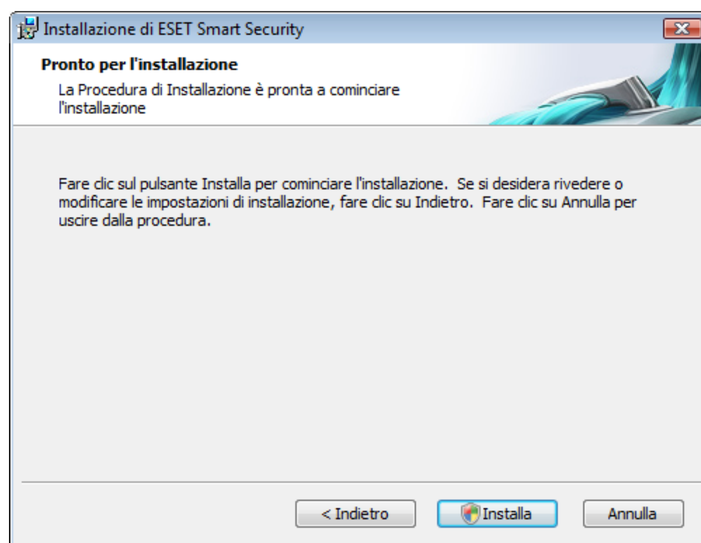
Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione **Rilevamento delle applicazioni potenzialmente indesiderate**. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose, tuttavia potrebbero influire negativamente sul comportamento del sistema operativo.

Applicazioni di questo tipo spesso fanno parte dell'istallazione di altri programmi e può essere difficile notarle durante l'istallazione. In genere viene, infatti, visualizzata una notifica durante l'installazione di queste applicazioni, ma è frequente il caso di applicazioni installate senza il consenso dell'utente.



Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET Smart Security di rilevare questo tipo di minaccia (scelta consigliata).

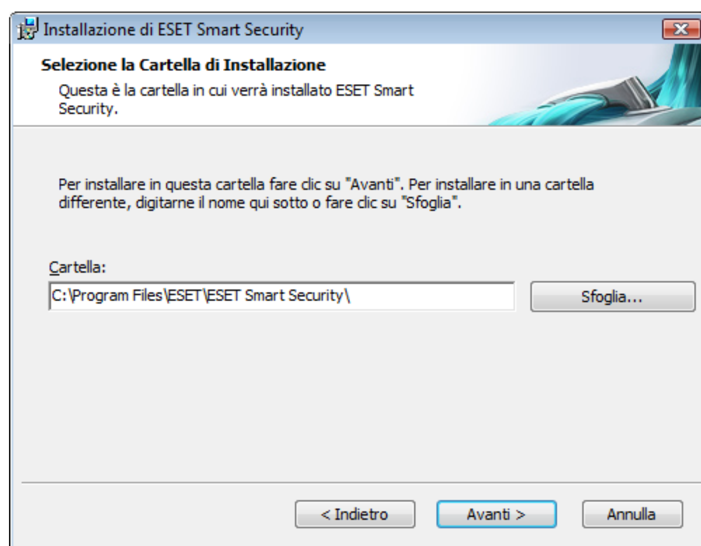
L'ultimo passaggio dell'installazione tipica è la conferma dell'installazione con il pulsante **Installa**.



2.2 Installazione personalizzata

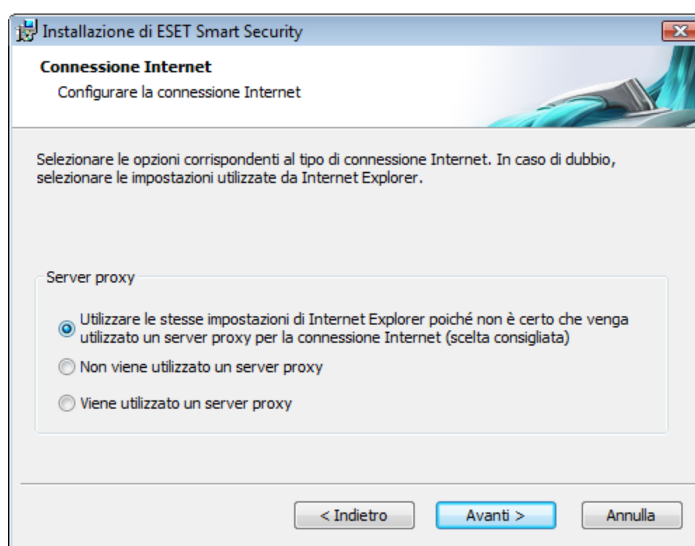
L'installazione **personalizzata** è indicata per utenti con esperienza nella configurazione dettagliata dei programmi e che desiderano modificare le impostazioni avanzate durante l'installazione.

La prima operazione da eseguire consiste nel selezionare il percorso della cartella di installazione. Per impostazione predefinita, il programma viene installato nella cartella C:\Programmi\ESET\ESET Smart Security\. Nell'specificare un percorso diverso, scegliere **Sfoglia...** (scelta non consigliata).

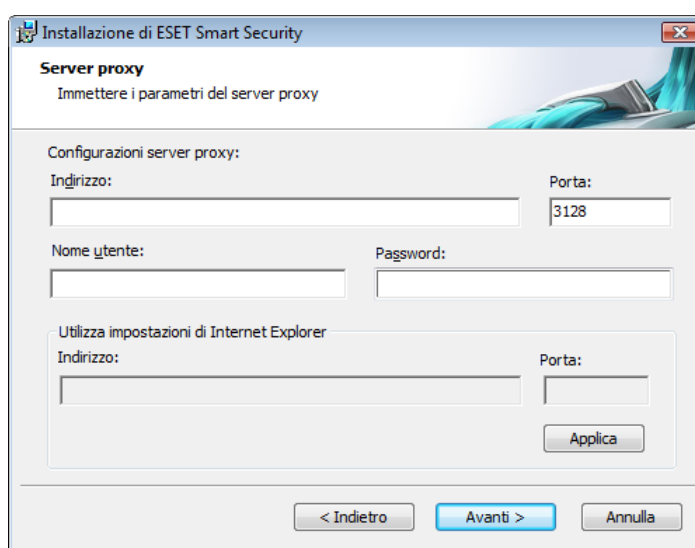


Quindi **immettere nome utente e password**. Questo passaggio è analogo a quello dell'installazione tipica (vedere a pagina 6).

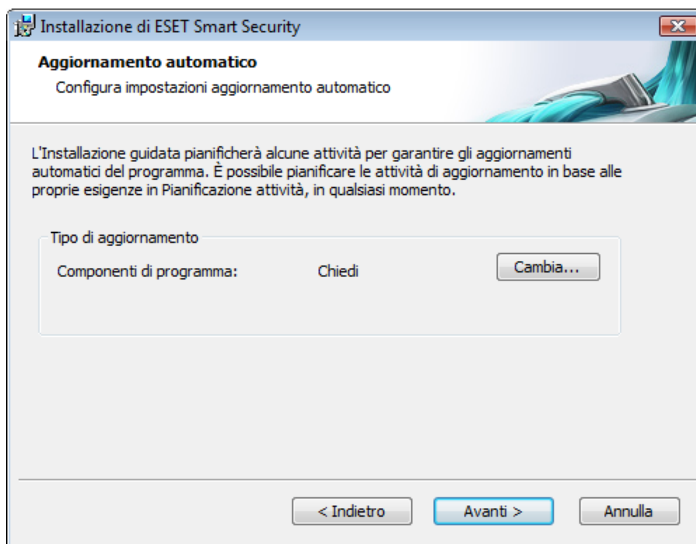
Dopo aver immesso nome utente e password, fare clic su **Avanti** per **Configurare la connessione Internet**.



Se si utilizza un server proxy, questo deve essere configurato in modo corretto per consentire la ricezione degli aggiornamenti delle firme antivirali. Se non si è certi dell'utilizzo di un server proxy per la connessione a Internet, selezionare **Utilizzare le stesse impostazioni di Internet Explorer poiché non è certo che venga utilizzato un server proxy per la connessione Internet (scelta consigliata)**, quindi scegliere **Avanti**. Se non si utilizza un server proxy, selezionare l'opzione corrispondente.

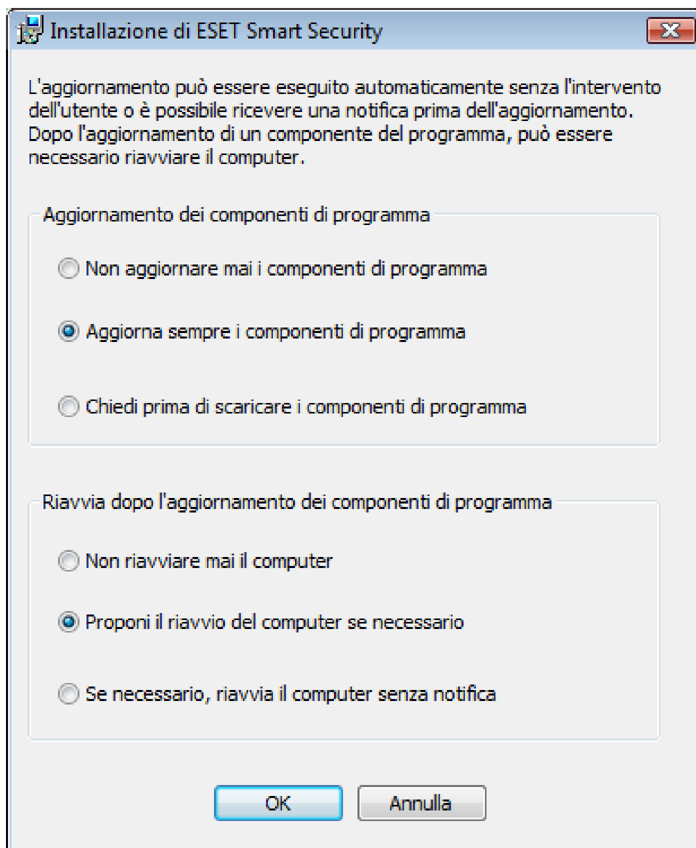


Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy** e scegliere **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo.** Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Se il server proxy richiede l'autenticazione, sarà necessario immettere un nome utente e una password validi per consentire l'accesso al server proxy. Se si desidera è possibile anche copiare le impostazioni del server proxy da Internet Explorer. A tal fine, scegliere **Applica** e confermare la selezione.



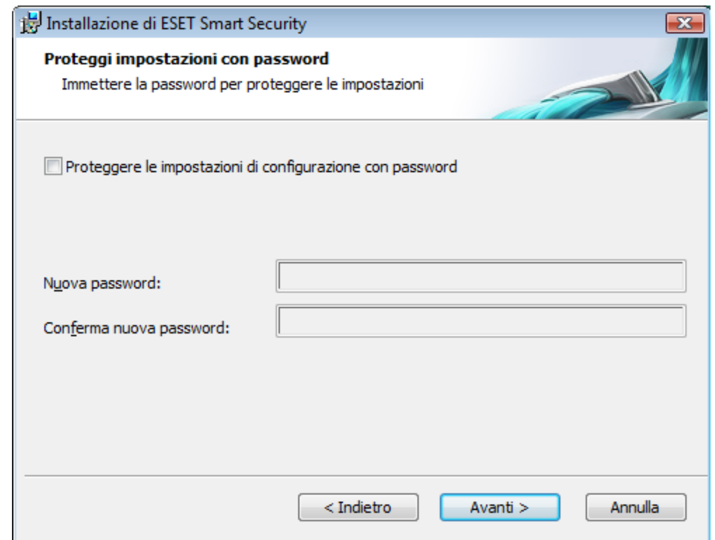
Fare clic su **Avanti** per passare alla finestra **Configura impostazioni aggiornamento automatico**. In questa fase è possibile specificare come si desidera che vengano gestiti gli aggiornamenti automatici dei componenti di programma sul sistema. Scegliere **Cambia...** per accedere alle impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare **Non aggiornare mai i componenti di programma**. L'opzione **Chiedi prima di scaricare i componenti di programma** consente di visualizzare una finestra di conferma prima di scaricare i componenti di programma. Per attivare l'aggiornamento automatico dei componenti di programma, selezionare l'opzione **Esegui l'aggiornamento dei componenti di programma se disponibili**.



NOTA: dopo l'aggiornamento di un componente del programma, è in genere necessario riavviare il sistema. L'impostazione consigliata è: **Se necessario, riavvia il computer senza notifica**.

Il passaggio successivo dell'istallazione consiste nell'inserimento di una password per proteggere i parametri del programma. Scegliere una password con la quale si desidera proteggere il programma. Inserire nuovamente la password per conferma.



I passaggi di **Configurazione del Sistema di allarme immediato (ThreatSense.Net)** e **Rilevamento delle applicazioni potenzialmente indesiderate** sono analoghi a quelli dell'Installazione tipica e non vengono riportati qui (vedere a pagina 6).

L'ultimo passaggio della modalità Personalizzata consiste nella selezione della modalità di filtro del Firewall ESET. Sono disponibili cinque modalità:

- Automatica
- Modalità automatica con eccezioni (regole definite dall'utente)
- Interattiva
- Basata su criteri
- Riconoscimento



La modalità **Automatica** è consigliata per la maggior parte degli utenti. Tutte le connessioni standard in uscita sono abilitate (analizzate automaticamente con le impostazioni predefinite), mentre le connessioni in entrata non desiderate vengono automaticamente bloccate.

Modalità automatica con eccezioni (regole definite dall'utente). La modalità automatica consente inoltre di aggiungere regole personalizzate.

La modalità **Interattiva** è adatta agli utenti esperti. Le comunicazioni vengono gestite mediante regole definite dall'utente. In caso di assenza di regole definite per le comunicazioni, verrà richiesto all'utente se consentire o rifiutare la comunicazione.

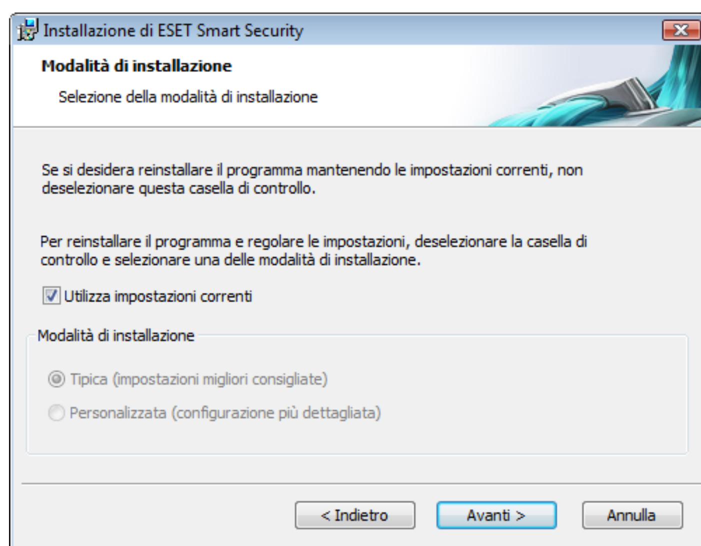
La modalità **Basata su criteri** valuta le comunicazioni in base a regole predefinite create dall'amministratore. In caso di assenza di regole disponibili, la connessione verrà automaticamente bloccata e all'utente non sarà visualizzato alcun messaggio di allarme. È consigliabile selezionare la modalità basata sui criteri solo nel caso in cui l'utente sia un amministratore che intende configurare le comunicazioni di rete.

Modalità riconoscimento - Crea e salva automaticamente le regole, inoltre, è ideale per la configurazione iniziale del firewall. Non è richiesta alcuna interazione utente, poiché ESET Smart Security esegue il salvataggio seguendo parametri predefiniti. Modalità riconoscimento non è una modalità protetta, pertanto è consigliabile utilizzarla solo fintanto che non si siano create tutte le regole richieste per le comunicazioni.

L'ultimo passaggio mostra una finestra che richiede il consenso per l'installazione.

2.3 Utilizzo delle impostazioni originali

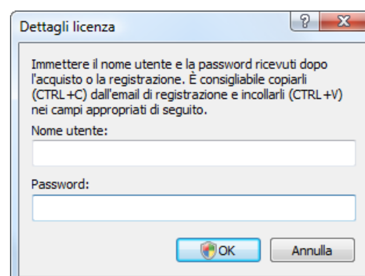
Quando si reinstalla ESET Smart Security, viene visualizzata l'opzione **Utilizza impostazioni correnti**. Selezionare questa opzione per trasferire i parametri di configurazione dall'installazione originale alla nuova.



2.4 Inserimento di nome utente e password

Per garantire una funzionalità ottimale è di fondamentale importanza che il programma venga aggiornato automaticamente. Ciò è possibile solo se il nome utente e la password vengono immessi correttamente nella configurazione dell'aggiornamento.

Se nome utente e password non sono stati immessi durante l'installazione, è possibile farlo a questo punto. Nella finestra principale del programma scegliere **Aggiorna**, quindi **Impostazione nome utente e password...** Immettere nella finestra **Dettagli licenza** i dati ricevuti con la licenza del prodotto.



2.5 Controllo computer su richiesta

Dopo l'installazione di ESET Smart Security, è opportuno eseguire un controllo del computer per rilevare l'eventuale presenza di codice dannoso. Per avviare rapidamente un controllo, selezionare **Controllo computer** nella finestra principale del programma, quindi scegliere **Controllo standard**. Per ulteriori informazioni sulla funzionalità di controllo del computer, vedere il capitolo "Controllo del computer".



3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET Smart Security e sulle configurazioni di base.

3.1 Introduzione all'interfaccia utente: modalità

La finestra principale di ESET Smart Security è suddivisa in due sezioni principali. Nella colonna a sinistra è possibile accedere al menu principale di facile utilizzo. La finestra principale del programma sulla destra ha come funzione primaria la visualizzazione delle informazioni che corrispondono all'opzione selezionata nel menu principale.

Di seguito è riportata una descrizione dei pulsanti del menu principale:

Stato protezione: in un formato di facile lettura, sono riportate informazioni sullo stato di protezione di ESET Smart Security. Se è attivata la modalità avanzata, verrà visualizzato lo stato di tutti i moduli di protezione. Fare clic su un modulo per visualizzarne lo stato corrente.

Controllo computer: in questa sezione l'utente può configurare e avviare il controllo del computer su-richiesta.

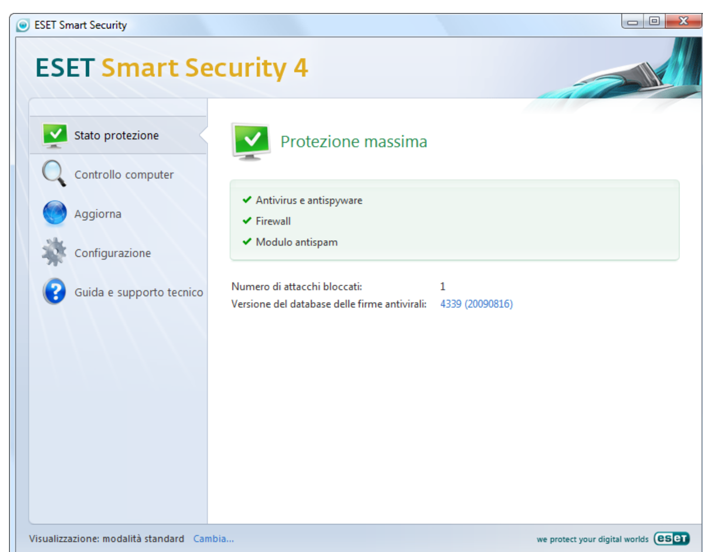
Aggiorna: selezionare questa opzione per accedere al modulo di aggiornamento con cui gestire gli aggiornamenti del database delle firme antivirali.

Configurazione: selezionare questa opzione per regolare il livello di protezione del computer. Se è attivata la modalità avanzata, verranno visualizzati i sottomenu dei moduli Protezione antivirus e antispyware, Personal firewall e Antispam.

Strumenti: questa opzione è disponibile solo in modalità avanzata. Consente di accedere ai file di raporto e alle informazioni su quarantena e pianificazione.

Guida e supporto tecnico: selezionare questa opzione per accedere ai file della guida, alla Knowledgebase di ESET, al sito Web di ESET e alle richieste di supporto tecnico.

L'interfaccia utente di ESET Smart Security consente agli utenti di alternare le modalità Standard e Avanzata. Per passare da una modalità all'altra, cercare il collegamento **Visualizza** nell'angolo inferiore sinistro della schermata principale di ESET Smart Security. Fare clic su questo pulsante per selezionare la modalità di visualizzazione desiderata.



La modalità standard consente l'accesso alle funzioni necessarie per le normali operazioni. Tale modalità non visualizza opzioni avanzate.

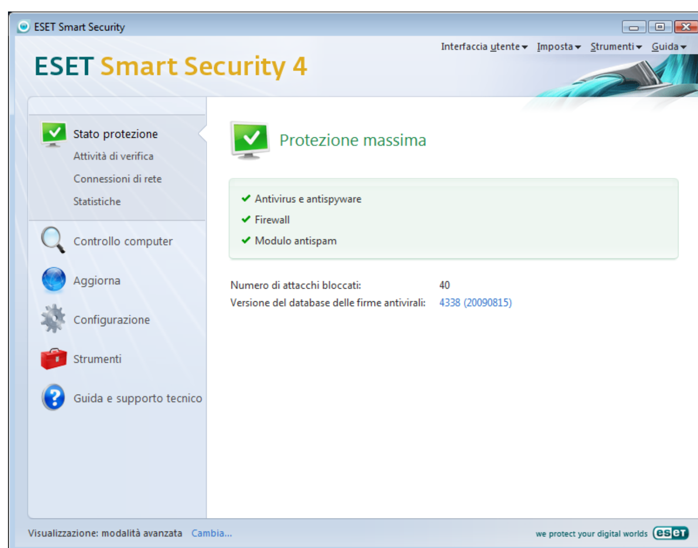


Quando si passa alla modalità avanzata, viene aggiunta l'opzione **Strumenti** al menu principale. L'opzione Strumenti consente all'utente di accedere a Pianificazione attività, Quarantena o visualizzare i File di rapporto di ESET Smart Security.

NOTA: tutte le istruzioni rimanenti della guida si riferiscono alla modalità avanzata.

3.1.1 Verifica del funzionamento del sistema

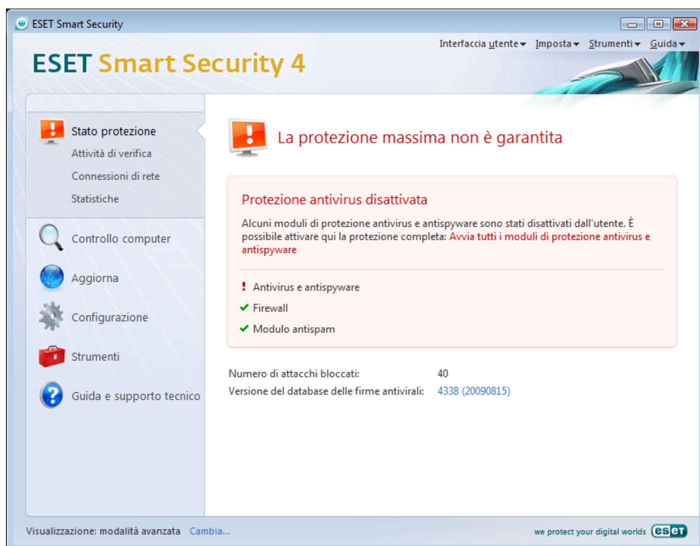
Per visualizzare lo **Stato protezione**, fare clic su questa opzione nella parte superiore del menu principale. Sul lato destro della finestra verrà visualizzato un rapporto sul funzionamento di ESET Smart Security con un sottomenu con tre voci: **Antivirus e antispyware**, **Personal firewall** e **Modulo antispam**. Selezionare uno di questi elementi per visualizzare informazioni dettagliate su uno specifico modulo di protezione.



Se i moduli attivati funzionano correttamente, verrà mostrato un indicatore di colore verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione e, nella parte superiore della finestra, verranno mostrate ulteriori informazioni sul modulo che presenta dei problemi. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul modulo desiderato.

3.1.2 Cosa fare se il programma non funziona correttamente

Se ESET Smart Security rileva un problema in alcuni moduli di protezione, il problema verrà segnalato nella finestra **Stato protezione**, nella quale viene inoltre proposta una potenziale soluzione del problema.

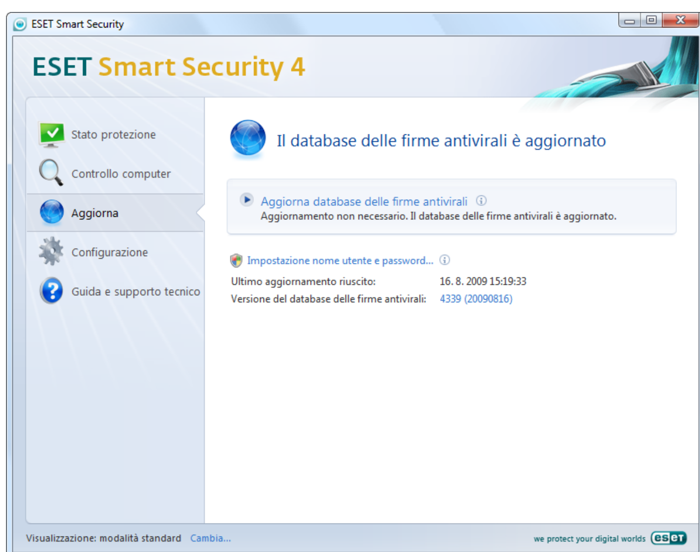


Nel caso in cui non sia possibile risolvere il problema ricorrendo all'elenco di problemi e soluzioni noti e descritti, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida o eseguire una ricerca nella Knowledgebase. Se non si riesce comunque a trovare una soluzione, è possibile inviare una richiesta di assistenza al supporto tecnico di ESET. In base ai commenti e ai suggerimenti degli utenti, gli specialisti di ESET possono rispondere rapidamente alle domande degli utenti e proporre delle soluzioni per i problemi.

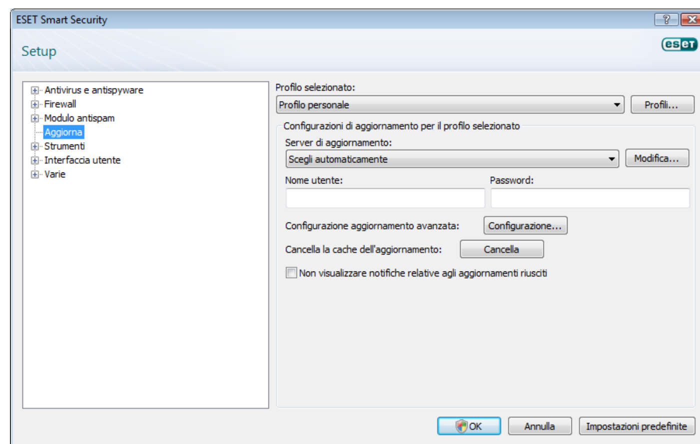
3.2 Configurazione dell'aggiornamento

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla configurazione e al funzionamento dell'aggiornamento. Nel menu principale selezionare **Aggiorna**, quindi fare clic su **Aggiorna database delle firme antivirali** nella finestra principale del programma per verificare immediatamente la disponibilità di un aggiornamento del database. **Impostazione nome utente e password...** consente di visualizzare la finestra di dialogo in cui immettere il nome utente e la password ricevuti al momento dell'acquisto.

Se nome utente e password sono stati specificati durante l'installazione di ESET Smart Security, questa finestra di dialogo non verrà visualizzata.

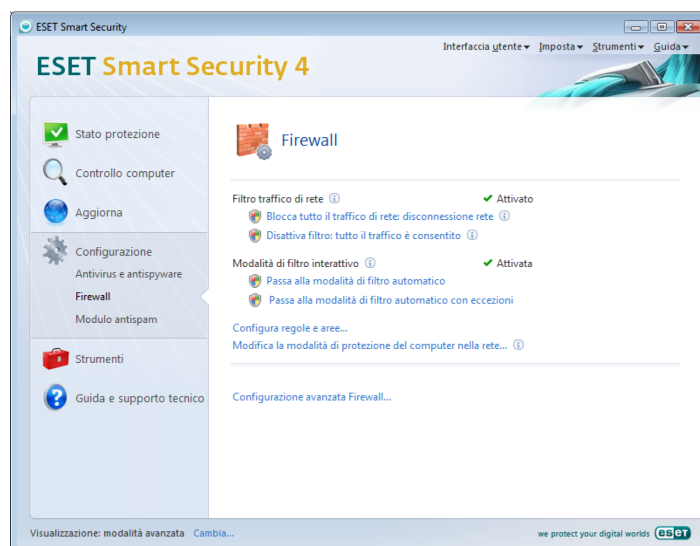


Nella finestra **Configurazione avanzata** (per accedere, premere F5) sono disponibili altre opzioni dettagliate per l'aggiornamento. Il menu a discesa **Server di aggiornamento:** deve essere impostato su **Scegli automaticamente**. Per configurare le opzioni di aggiornamento avanzate, tra cui la modalità di aggiornamento, l'accesso al server proxy, l'accesso agli aggiornamenti su un server locale e la creazione di copie delle firme antivirali (in ESET Smart Security Business Edition), fare clic sul pulsante **Configurazione**.



3.3 Impostazione area attendibile

La configurazione di un'area sicura costituisce un aspetto importante della protezione del computer in un ambiente di rete. Attraverso la configurazione dell'area sicura e della condivisione è possibile consentire l'accesso al computer ad altri utenti. Fare clic su **Configurazione > Personal firewall > Modifica la modalità di protezione del computer nella rete**. Verrà visualizzata una finestra che consente di configurare le impostazioni della modalità di protezione del computer nella rete/area effettiva.



Il rilevamento dell'area sicura e affidabile viene eseguito dopo l'installazione di ESET Smart Security o dopo la connessione del computer a una nuova rete. In molti casi non è, pertanto, necessario definire l'Area sicura. Nell' impostazione predefinita, al rilevamento di una nuova area verrà visualizzata una finestra di dialogo che consente di impostare il livello di protezione per l'area.

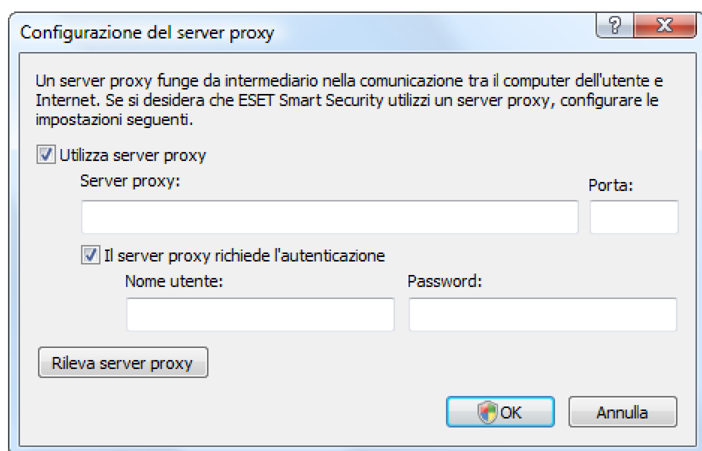


Avviso! Una configurazione dell'area sicura non corretta potrebbe costituire un rischio per la protezione del computer.

NOTA: Nell' impostazione predefinita, le workstation di una rete sicura possono accedere a file e stampanti condivisi; è attivata, inoltre, la comunicazione RPC in entrata ed è disponibile la condivisione del desktop remoto.

3.4 Impostazione del server proxy

Se per mediare la connessione a Internet su un sistema che utilizza ESET Smart Security si utilizza un server proxy, questo deve essere specificato nella Configurazione avanzata. Per accedere alla finestra di configurazione del **Server proxy**, scegliere **Varie > Server proxy** dalla struttura Configurazione avanzata. Selezionare la casella di controllo **Utilizza server proxy**, quindi immettere l'indirizzo IP e la porta del server proxy, oltre ai dati di autenticazione.



Nel caso in cui queste informazioni non siano disponibili, è possibile tentare di rilevare automaticamente le impostazioni del server proxy per ESET Smart Security facendo clic sul pulsante **Rileva server *proxy***.

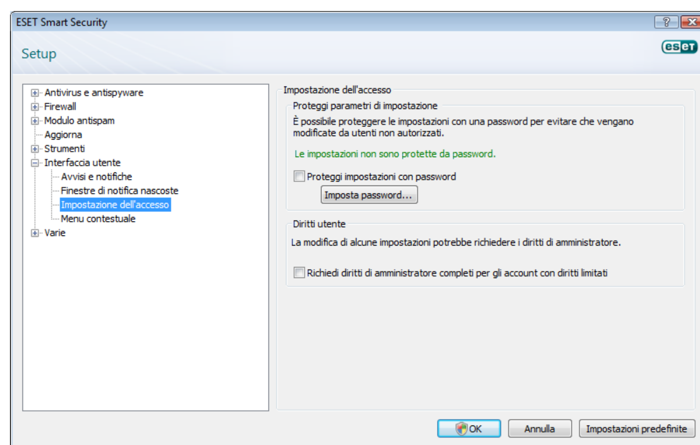
NOTA: le opzioni del server proxy potrebbero essere diverse in base ai diversi profili di aggiornamento. In questo caso, configurare il server proxy nella Configurazione aggiornamento avanzata.

3.5 Configurazione protezione

La configurazione di ESET Smart Security riveste una grande rilevanza dal punto di vista dei criteri di sicurezza dell'organizzazione di appartenenza.

Le modifiche non autorizzate possono mettere a rischio la stabilità e la protezione del sistema. Per proteggere con una password i parametri di configurazione, nel menu principale fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa... > Interfaccia utente > Protezione impostazioni** e fare clic sul pulsante **Immetti password...**

Immettere una password, confermarla immettendola di nuovo, quindi scegliere **OK**. Questa password verrà richiesta per tutte le modifiche future alle impostazioni di ESET Smart Security.



4. Utilizzo di ESET Smart Security

4.1 Protezione antivirus e antispyware

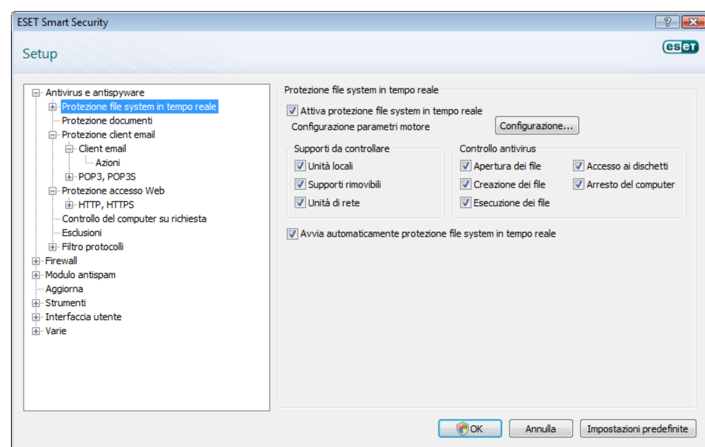
La protezione antivirus difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla: prima bloccandola e poi disinfettandola, eliminandola o mettendola in quarantena.

4.1.1 Protezione del file system in tempo reale

La funzione di protezione del file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus del sistema. Tutti i file vengono controllati alla ricerca di codice dannoso nel momento in cui vengono aperti, creati o eseguiti sul computer. La funzione di protezione del file system in tempo reale viene avviata all'avvio del sistema.

4.1.1.1 Impostazione del controllo

La protezione del file system in tempo reale prevede il controllo di tutti i tipi di supporto quando si verificano determinati eventi. Il controllo utilizza i metodi di rilevamento della tecnologia ThreatSense (come descritto in Configurazione parametri del motore ThreatSense). Il funzionamento del controllo può essere diverso ad esempio per i file appena creati e i file già esistenti. Nel caso di file appena creati è possibile applicare un livello di controllo maggiore.



4.1.1.1.1 Oggetti da controllare

Nell'impostazione predefinita, vengono controllati alla ricerca di potenziali minacce tutti i tipi di supporto.

Unità locali: controllo di tutte le unità disco rigido locali

Supporti rimovibili: dischetti, dispositivi di memorizzazione USB e così via

Unità di rete: controllo di tutte le unità mappate

È consigliabile mantenere le impostazioni predefinite e modificare tali impostazioni solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

4.1.1.1.2 Scansione (scansione quando si verifica un evento)

Nell'impostazione predefinita, tutti i file vengono controllati all'apertura, durante l'esecuzione o la creazione. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

L'opzione Accesso ai dischetti garantisce il controllo del settore di avvio del dischetto durante l'accesso all'unità. L'opzione **Arresto del computer** garantisce il controllo dei settori di avvio del disco rigido durante l'arresto del computer. Sebbene i virus del settore di avvio siano oggi piuttosto rari, è consigliabile lasciare attivata questa opzione, poiché esiste ancora la possibilità di infezione di un virus del settore di avvio da fonti alternative.

4.1.1.1.3 Parametri ThreatSense aggiuntivi per i file appena creati e modificati

La probabilità di infezione nei file appena creati è maggiore in confronto ai file già esistenti. Per questo motivo il programma controlla i nuovi file con parametri di controllo aggiuntivi. Insieme ai comuni metodi di controllo basati sulle firme, viene utilizzata l'euristica avanzata, che consente un notevole miglioramento delle percentuali di rilevamento. Oltre ai file appena creati, il controllo viene eseguito anche sui file autoestraenti (SFX) e sugli eseguibili compressi (file eseguibili compressi internamente). Nell'impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e indipendentemente dalla loro dimensione effettiva. Deselezionare l'opzione ***Impostazioni di controllo dell'archivio predefinito*** per modificare le impostazioni di scansione dell'archivio.

4.1.1.1.4 Configurazione avanzata

Nell'garantire un impatto minimo sul sistema durante l'uso della protezione in tempo reale, il controllo dei file già esaminati non viene eseguito di nuovo (a meno che i file non siano stati modificati). I file vengono controllate nuovamente subito dopo ogni aggiornamento del database di firme antivirali. Questo comportamento viene configurato con l'opzione **Attività di controllo ottimizzata**. Quando questa funzione è disattivata, tutti i file vengono controllati a ogni accesso.

Per impostazione predefinita, la protezione in tempo reale viene avviata automaticamente all'avvio del sistema operativo e procede a un controllo continuo. In casi particolari (ad esempio, in caso di conflitto con un altro programma di controllo in tempo reale), la protezione in tempo reale può essere arrestata disattivando l'opzione **Avvio automatico della protezione file system in tempo reale**.

Per impostazione predefinita l'euristica avanzata non viene utilizzata quando i file vengono eseguiti. Tuttavia, in alcuni casi questa opzione può essere attivata selezionando l'opzione **Euristica avanzata all'esecuzione dei file**. È possibile che l'euristica avanzata rallenti l'esecuzione di alcuni programmi a causa dell'aumento dei requisiti di sistema.

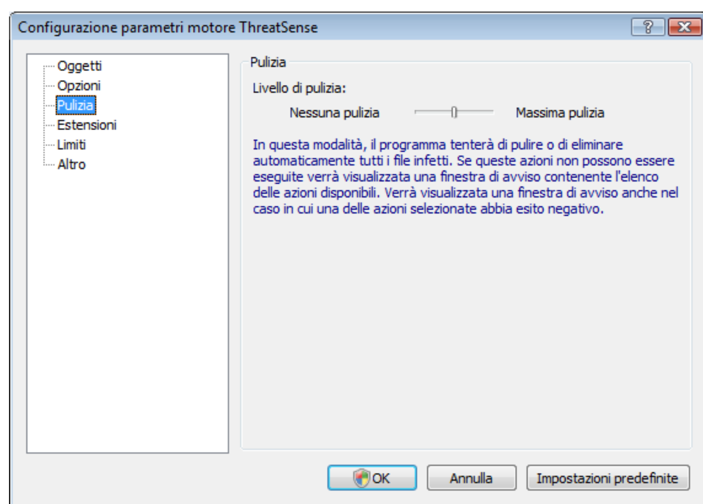
4.1.1.2 Livelli di pulitura

La protezione in tempo reale prevede tre livelli di pulizia (per accedere alle impostazioni, fare clic sul pulsante **Configurazione...** nella sezione **Protezione file system in tempo reale**, quindi fare clic su **Pulizia**).

- Il primo livello visualizza una finestra di avviso con le opzioni disponibili per ciascuna infiltrazione rilevata. L'utente deve scegliere l'azione più adatta a ciascuna infiltrazione. Questo livello è indicato per utenti più esperti, che conoscono le azioni più adatte da intraprendere per tutti i tipi di infiltrazione.

- Il livello predefinito prevede la selezione ed esecuzione automatica di un'azione predefinita (in base al tipo di infiltrazione). Un messaggio nell'angolo inferiore destro della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Non viene, tuttavia, eseguita un'azione automatica nel caso in cui l'infiltrazione si trovi in un archivio che contiene anche file puliti, come pure non viene eseguita su oggetti per i quali non è prevista un'azione predefinita.

- Il terzo livello è il più "aggressivo" e prevede la pulizia di tutti gli oggetti infetti. Questo livello potrebbe portare alla perdita di file validi ed è pertanto consigliabile utilizzarlo solo in situazioni specifiche.



4.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. È pertanto necessario prestare attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici, ad esempio quando si verifica un conflitto con una determinata applicazione o con il controllo in tempo reale di un altro programma antivirus.

Dopo l'installazione di ESET Smart Security, tutte le impostazioni sono ottimizzate per offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic sul pulsante **Configurazioni predefinite** presente nell'angolo inferiore destro della finestra **Protezione file system in tempo reale** (**Configurazione avanzata > Antivirus e antispyware > Protezione file system in tempo reale**).

4.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo, speciale, rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. È scaricabile dal sito all'indirizzo http://www.eicar.org/download/eicar.com

NOTA: prima di eseguire un controllo della protezione in tempo reale, è necessario disattivare il firewall. Se resta attivato, rileverà e impedirà di scaricare i file di test.

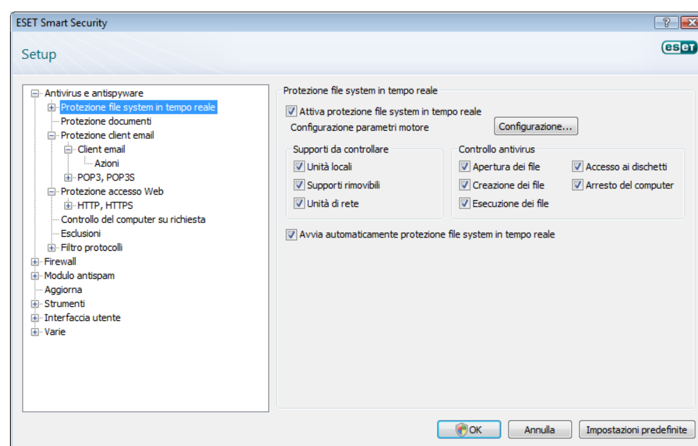
4.1.1.5 Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrati dei problemi che si verificano quando si utilizza la protezione in tempo reale e verrà descritto come risolverli.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione > Antivirus e antispyware** quindi scegliere **Attiva** nella sezione **Protezione file system in tempo reale** della finestra principale del programma.

Se la protezione in tempo reale non viene eseguita all'avvio del sistema, è probabile che l'opzione **Avvio automatico della protezione file system in tempo reale non sia attivata**. Per attivare l'opzione, selezionare **Configurazione avanzata** (F5) e fare clic su **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Nella sezione **Configurazione avanzata** alla fine della finestra, accertarsi che la casella di controllo **Avvio automatico della protezione file system in tempo reale** sia selezionata.



La protezione in tempo reale non rileva e pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se attivati contemporaneamente, due scudi di protezione in tempo reale possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene eseguita all'avvio del sistema (e l'opzione **Avvio automatico della protezione file system in tempo reale** è attivata), il motivo può essere il conflitto con altri programmi. In questo caso, consultare gli specialisti del Supporto tecnico di ESET.

4.1.2 Protezione client e-mail

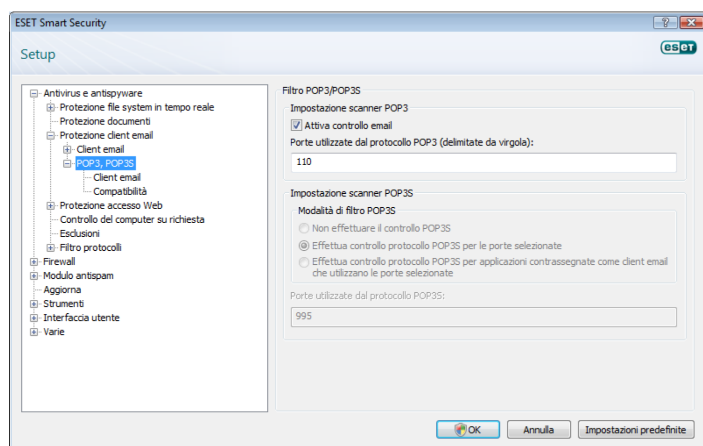
La protezione email garantisce il controllo delle comunicazioni via email ricevute mediante il protocollo POP3. Utilizzando il plug-in per Microsoft Outlook, ESET Smart Security controlla tutte le comunicazioni dal client email (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, vengono utilizzati tutti i metodi di scansione avanzata forniti dal motore di scansione ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database di firme antivirali. La scansione delle comunicazioni mediante protocollo POP3 non dipende dal client e-mail utilizzato.

4.1.2.1 Controllo POP3

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client e-mail. ESET Smart Security fornisce la protezione di questo protocollo indipendentemente dal client e-mail utilizzato.

Il modulo che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client e-mail. Nell'impostazione predefinita, vengono controllate tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

Le comunicazioni crittografate non vengono controllate.



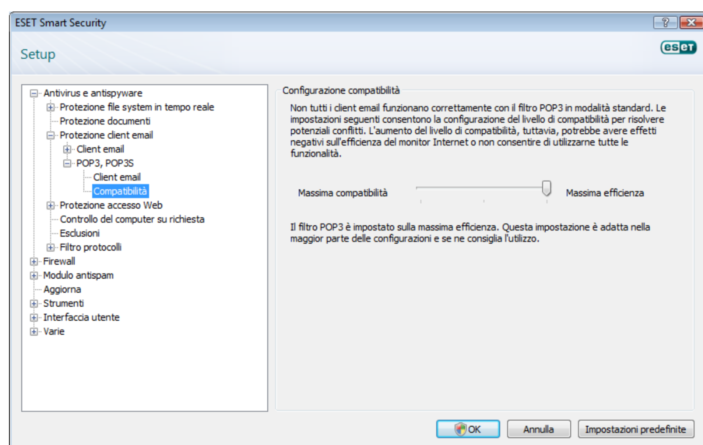
4.1.2.1.1 Compatibilità

Con alcuni programmi email è possibile che si verifichino dei problemi durante le operazioni di filtro POP3 (ad esempio, se si ricevono messaggi con una connessione a Internet lenta, possono verificarsi dei timeout a causa del controllo). In questo caso, provare a modificare la modalità di esecuzione del controllo. È possibile rendere il processo di disinfezione più veloce riducendo il livello di controllo. Per modificare il livello di controllo del filtro POP3, passare a **Antivirus e antispyware > Protezione email > POP3 > Compatibilità**.

Se si è attivata l'opzione **Massima efficienza**, le infiltrazioni vengono rimosse dai messaggi infetti (se le opzioni **Elimina** o **Pulisci** sono attivate o se è attivato il livello di disinfezione **massimo** o **predefinito**) e le informazioni sull'infiltrazione vengono inserite prima dell'oggetto originale del messaggio di email.

Media compatibilità modifica la modalità di ricezione dei messaggi. I messaggi vengono inviati al client email in modo graduale: una volta trasferita l'ultima parte del messaggio, questo verrà controllato alla ricerca di infiltrazioni. Tuttavia, il rischio di infezioni aumenta con questo livello di controllo. Il livello di disinfezione e la gestione delle notifiche (avvisi aggiunti alla riga dell'oggetto e al corpo dei messaggi di email) è identico all'impostazione di massima efficienza.

Con il livello **Massima compatibilità**, l'utente viene avvisato da una finestra di avviso che indica la ricezione di un messaggio infetto. Nessuna informazione sui file infetti viene aggiunta alla riga dell'oggetto o al corpo dell'e-mail dei messaggi recapitati e le infiltrazioni non vengono rimosse automaticamente. L'eliminazione delle infiltrazioni deve essere eseguita dall'utente direttamente dal client e-mail.

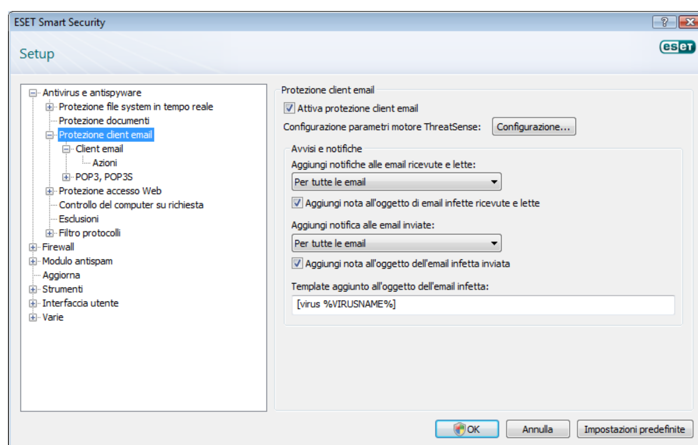


4.1.2.2 Integrazione con client e-mail

L'integrazione di ESET Smart Security con i client email aumenta il livello di protezione attiva contro codici dannosi nei messaggi email. L'integrazione può essere attivata in ESET Smart Security solo se il client email è supportato. Se è attivata l'integrazione, la barra degli strumenti Antispam di ESET Smart Security viene inserita direttamente nel client email, contribuendo ad aumentare la protezione delle comunicazioni via email. Le impostazioni di integrazione sono disponibili in **Configurazione > Immettere struttura di impostazione avanzata completa… > Varie > Integrazione con client email**. In questa finestra di dialogo è possibile attivare l'integrazione con i client email supportati. I client e-mail attualmente supportati comprendono Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird.

Selezionare l'opzione ***Disattiva il controllo alla modifica del contenuto della posta in arrivo*** se si presenta un rallentamento del sistema durante l'utilizzo del client e-mail. Una situazione simile può verificarsi durante il download dei messaggi e-mail da Kerio Outlook Connector Store.

La protezione email si avvia selezionando la casella di controllo **Attiva la protezione email** in **Configurazione avanzata** (F5) > **Antivirus e antispyware** > **Protezione email**.



4.1.2.2.1 Aggiunta di notifiche al corpo di un messaggio e-mail

È possibile contrassegnare ciascun messaggio email controllato da ESET Smart Security aggiungendo una notifica all'oggetto o al corpo del messaggio. Questa funzione aumenta l'attendibilità dei messaggi inviati ai destinatari e, se viene rilevata un'infiltrazione, fornisce informazioni utili sul livello di minaccia costituito dal mittente.

Le opzioni per questa funzione sono disponibili in **Configurazione avanzata > Antivirus e antispyware > Protezione client e-mail**. In ESET NOD32 Antivirus sono disponibili le funzioni **Aggiungi notifiche alle email ricevute e lette** e **Aggiungi notifica alle email inviate**. Gli utenti possono scegliere se aggiungere le note a tutti i messaggi email, solo ai messaggi infetti o a nessun messaggio. Con ESET Smart Security è inoltre possibile aggiungere delle note all'oggetto originale dei messaggi infetti. Per aggiungere delle note all'oggetto, utilizzare le opzioni **Aggiungi nota all'oggetto di email infette ricevute e lette** e **Aggiungi una nota all'oggetto di email infette inviate**.

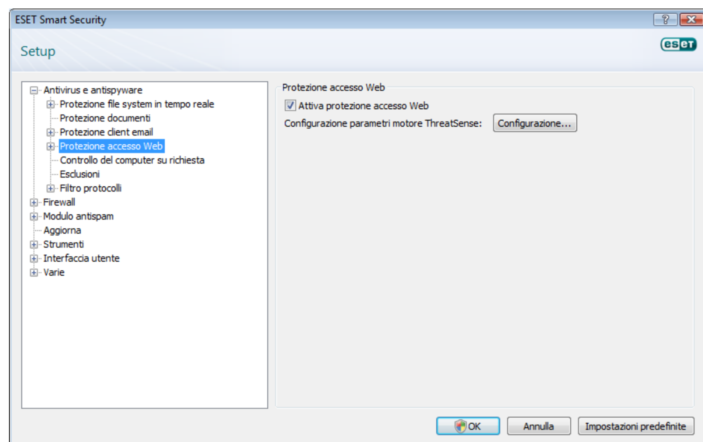
Il contenuto delle notifiche può essere modificato nel Template aggiunto all'oggetto dell'email infetta. Le modifiche menzionate consentono di automatizzare il processo di filtro dei messaggi email infetti, poiché questi messaggi vengono filtrati in una cartella a parte (se previsto dal client email in uso).

4.1.2.3 Eliminazione delle infiltrazioni

In caso di ricezione di messaggi e-mail infetti, verrà visualizzata una finestra di avviso con il nome del mittente, il messaggio e-mail e il nome dell'infiltrazione. Nella parte inferiore della finestra, sono disponibili le opzioni **Pulisci**, **Elimina** o **Nessuna azione** per l'oggetto rilevato. Nella maggior parte dei casi è consigliabile selezionare **Pulisci** o **Elimina**. In situazioni particolari in cui si desidera comunque ricevere il file infetto, selezionare **Nessuna azione**. Se è attivato il livello **Massima pulitura**, verrà visualizzata una finestra di informazioni, senza nessuna opzione disponibile per gli oggetti infetti.

4.1.3 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventata anche lo strumento principale per il trasferimento di codice dannoso. Per questo motivo, è essenziale considerare con attenzione la protezione dell'accesso al Web. È importante controllare che l'opzione **Attiva la protezione accesso Web** sia attivata. Per accedere a questa opzione, scegliere **Configurazione avanzata (F5) > Antivirus e antispyware > Protezione accesso Web**.



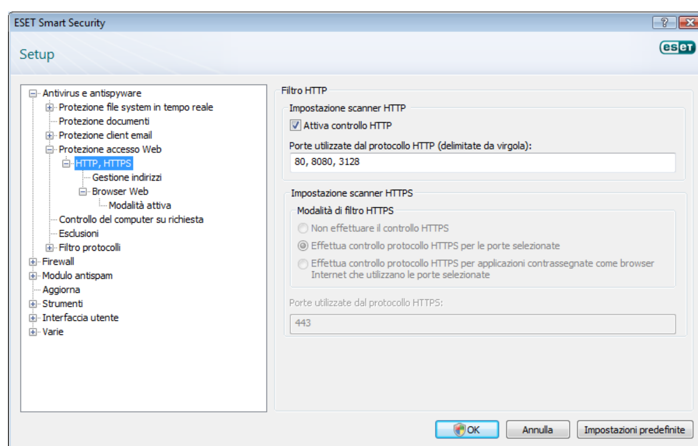
4.1.3.1 HTTP, HTTPS

La protezione dell'accesso al Web consiste prevalentemente nel controllo della comunicazione dei browser con server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata). Nell'impostazione predefinita, ESET Smart Security è configurato in modo da utilizzare gli standard della maggior parte dei browser Internet. Le opzioni di configurazione dello scanner HTTP possono, tuttavia, essere modificate in Protezione accesso Web > HTTP, HTTPS. Nella finestra principale del filtro HTTP è possibile selezionare o deselezionare l'opzione **Attiva controllo HTTP**. È anche possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. L'impostazione predefinita per i numeri delle porte è 80, 8080 e 3128. Il controllo HTTPS può essere impostato con le seguenti modalità:

Non utilizzare il controllo del protocollo HTTPS
La comunicazione crittografata non verrà controllata

Utilizza il controllo del protocollo HTTPS per le porte selezionate
Il controllo HTTPS viene utilizzato solo per le porte definite in Porte utilizzate dal protocollo HTTPS

Utilizza il controllo del protocollo HTTPS per le applicazioni contrassegnate come browser Internet che utilizzano le porte selezionate
Vengono controllate unicamente applicazioni specificate nella sezione relativa ai browser e che utilizzano le porte definite in ***Porte utilizzate dal protocollo HTTPS***.

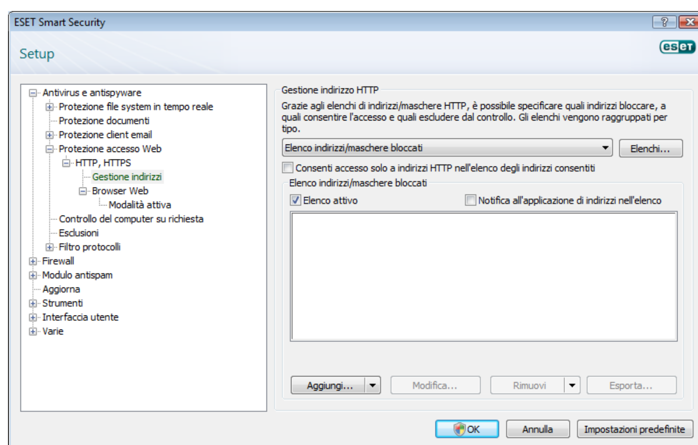


4.1.3.1.1 Gestione degli indirizzi

In questa sezione è possibile specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo.

I pulsanti **Aggiungi, Cambia, Rimuovi** e **Esporta vengono utilizzati per gestire l'elenco degli indirizzi**. Non sarà possibile accedere ai siti Web presenti nell'elenco degli indirizzi bloccati. Durante l'accesso i siti Web presenti nell'elenco degli indirizzi esclusi non vengono controllati per rilevare il codice dannoso. Se viene attivato ***Consenti accesso solo agli indirizzi HTTP dell'elenco indirizzi consentiti***, sarà possibile accedere solo agli indirizzi presenti nell'elenco degli indirizzi consentiti, mentre gli altri indirizzi HTTP verranno bloccati.

In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? L'asterisco sostituisce qualsiasi stringa di caratteri e il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Per attivare l'elenco, selezionare l'opzione ***Elenco attivo*** . Se si desidera ricevere una notifica quando viene immesso un indirizzo dall'elenco corrente, selezionare ***Notifica applicazione indirizzi dall'elenco.***

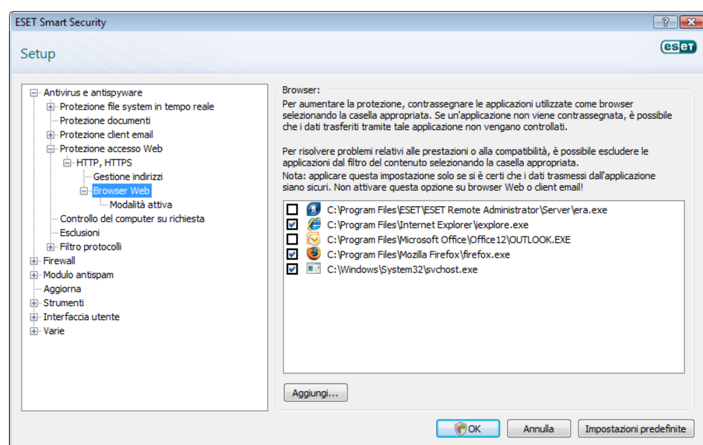


4.1.3.1.2 Browser

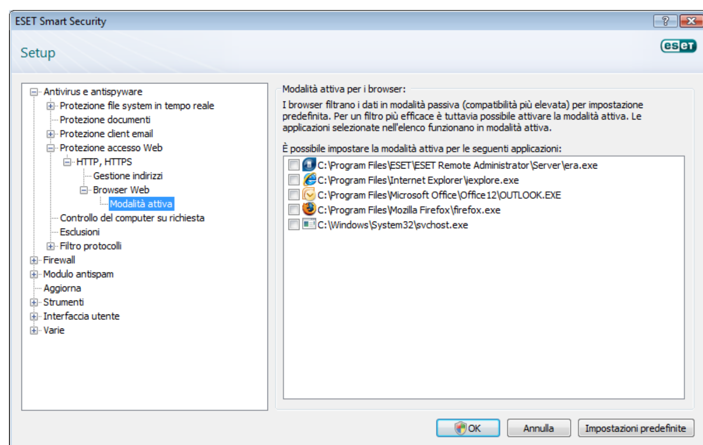
ESET Smart Security contiene inoltre la funzionalità **Browser**, che consente all'utente di stabilire se l'applicazione specificata è o non è un browser. Se un'applicazione è contrassegnata dall'utente come browser, tutte le comunicazioni di quest'applicazione verranno controlalte indipendentemente dal numero di porte coinvolte nella comunicazione.

La funzionalità Browser integra la funzione di controllo HTTP, in quanto quest'ultima funzione copre solo porte predefinite. Molti servizi Internet, tuttavia, utilizzano un numero sconosciuto o sempre diverso di porte. Per questo motivo la funzionalità Browser può stabilire

il controllo delle porte di comunicazione indipendentemente dai parametri di connessione.



L'elenco delle applicazioni contrassegnate come browser è accessibile direttamente dal sottomenu **Browser** della sezione **HTTP**. In questa sezione è presente anche il sottomenu **Modalità attiva** che definisce la modalità di controllo per i browser. La **Modalità attiva** è utile in quanto consente la verifica dell'insieme dei dati trasferiti. Se non è attivata, la comunicazione delle applicazioni viene monitorata gradualmente in batch. Questo può ridurre l'efficacia del processo di verifica dei dati, ma fornisce anche una maggiore compatibilità per le applicazioni elencate. Se non si verificano problemi durante l'utilizzo, è consigliabile attivare questa modalità di controllo selezionando la casella accanto all'applicazione desiderata.



4.1.4 Controllo del computer

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire un controllo del computer su richiesta per cercare eventuali infiltrazioni nel computer. Dal punto di vista della protezione, è essenziale che le scansioni del computer non vengano eseguite solo quando si sospetta un'infezione, ma regolarmente, come parte delle normali misure di protezione. Il controllo regolare garantisce il rilevamento delle infiltrazioni non rilevate dallo scanner in tempo reale quando sono state salvate sul disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è disattivato o quando il database di firme antivirali è obsoleto.

È consigliabile eseguire un controllo su richiesta almeno una o due volte al mese. La scansione può essere configurata come attività pianificata in **Strumenti > Pianificazione attività**.

4.1.4.1 Tipo di controllo

Sono disponibili due tipi di scansione: il **Controllo standard**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri, e il **Controllo personalizzato...**, che consente all'utente di selezionare uno dei profili predefiniti, oltre a scegliere oggetti da controllare dalla struttura.



4.1.4.1.1 Controllo standard

La scansione standard è un metodo di facile utilizzo che consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede una configurazione di scansione dettagliata. Con il controllo standard si controllano tutti i file presenti sulle unità locali e si puliscono o eliminano automaticamente le infiltrazioni trovate. Il livello di disinfezione viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di disinfezione, vedere la sezione corrispondente a pagina 20.

Il profilo di controllo standard è progettato per gli utenti che desiderano eseguire un controllo rapido e semplice del proprio computer. Infatti offre una soluzione di scansione e disinfezione efficace senza richiedere un lungo processo di configurazione.

4.1.4.1.2 Controllo personalizzato

Il controllo personalizzato è una soluzione ottimale quando si desidera specificare parametri quali destinazioni e metodi di controllo. Il vantaggio del controllo personalizzato è la possibilità di configurare i parametri in dettaglio. Questi profili sono particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri definiti dall'utente.

Per selezionare gli oggetti da controllare, utilizzare il menu a discesa per la selezione rapida dell'oggetto o selezionarli tra tutti i dispositivi disponibili nel computer. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione... > Pulizia**. Se si desidera eseguire solo il controllo del sistema senza eseguire altre operazioni, selezionare la casella di controllo **Controllo senza rimozione**.

L'esecuzione di controlli del computer mediante la modalità di controllo personalizzata è un'operazione adatta a utenti esperti con precedenti esperienze di utilizzo di programmi antivirus.

4.1.4.2 Oggetti da controllare

Il menu Oggetti da controllare consente di selezionare file, cartelle e dispositivi da controllare alla ricerca di virus.

Utilizzando l'opzione del menu di scelta rapida Oggetti da controllare, è possibile selezionare le seguenti destinazioni:

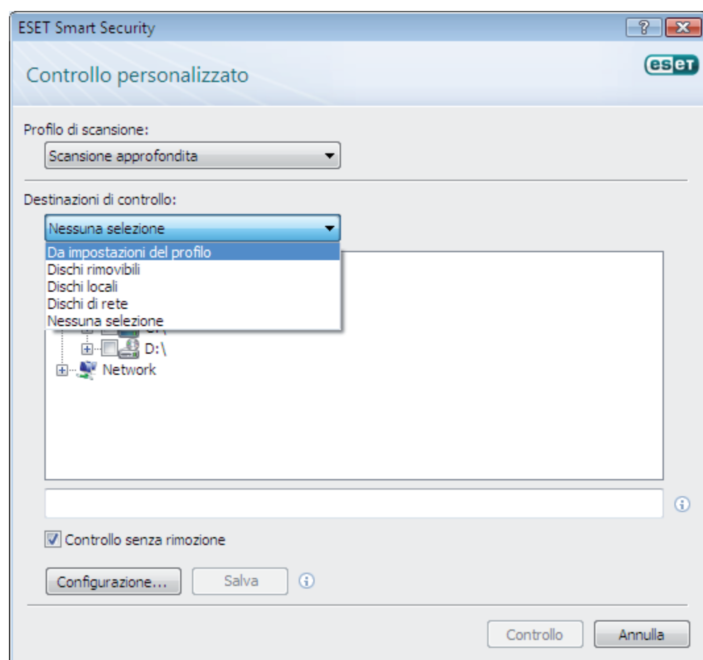
Per impostazioni profilo: consente di utilizzare le destinazioni specificate nel profilo selezionato

Supporti rimovibili: dischetti, dispositivi di memorizzazione USB, CD/DVD

Unità locali: controllo di tutte le unità disco rigido locali

Unità di rete: tutte le unità mappate

Nessuna selezione: consente di annullare tutte le selezioni



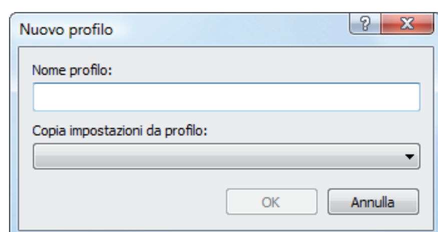
Una destinazione di controllo può anche essere specificata in modo più preciso, immettendo il percorso alla cartella dei file che si desidera includere nel controllo. Selezionare le destinazioni dalla struttura con tutti i dispositivi disponibili nel computer.

4.1.4.3 Profili di scansione

I parametri preferiti di controllo del computer possono essere salvati nei profili di scansione. Il vantaggio di creare profili di scansione è costituito dalla possibilità di utilizzarli regolarmente per le scansioni future. È consigliabile creare un numero di profili di scansione (con diverse destinazioni di scansione, metodi di scansione e altri parametri) pari a quelli utilizzati regolarmente dall'utente.

Per creare un nuovo profilo da utilizzare più volte per i controlli futuri, selezionare **Configurazione avanzata (F5) > Controllo computer su richiesta**. Fare clic sul pulsante **Profili...** sulla destra per visualizzare l'elenco di profili di controllo esistenti e l'opzione per la creazione di un nuovo profilo. **Impostazione parametri motore ThreatSense** descrive ciascun parametro di configurazione della scansione. Sarà utile per creare un profilo di scansione adatto alle proprie esigenze.

Esempio:
Si supponga di dover creare un proprio profilo di controllo e che la configurazione assegnata al profilo **Smart Scan** sia adatta almeno in parte. Tuttavia non si desidera eseguire il controllo di eseguibili compressi o di applicazioni potenzialmente pericolose, ma si desidera applicare l'opzione **Massima pulitura**. Nella finestra **Profili di configurazione** scegliere il pulsante **Aggiungi...** Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi scegliere **Smart scan** dal menu a discesa **Copia impostazioni da profilo.** Specificare quindi gli altri parametri in base alle proprie esigenze.



4.1.5 Filtro dei protocolli

La protezione antivirus per i protocolli di applicazioni POP3 e HTTP viene eseguita dal motore di scansione di ThreatSense, che integra perfettamente tutte le tecniche di scansione avanzata dei virus disponibili. Il controllo funziona automaticamente indipendentemente dal browser o dal client e-mail utilizzato. Per il filtro dei protocolli sono disponibili le opzioni seguenti (quando l'opzione **Attiva filtro del contenuto del protocollo di applicazioni** è abilitata):

Porte HTTP e POP3: consente di limitare la scansione delle comunicazioni a porte HTTP e POP3 conosciute.

Applicazioni contrassegnate come browser e client e-mail: attivare questa opzione per filtrare solo le comunicazioni di applicazioni contrassegnare come browser (Protezione accesso Web > HTTP, HTTPS > Browser) e client e-mail (Protezione client e-mail > POP3, POP3S > Client e-mail)

Porte e applicazioni contrassegnate come browser Internet o client email: viene effettuato il controllo malware sia sulle porte che sui browser

Nota:
A partire da Windows Vista Service Pack 1 e Windows Server 2008, viene utilizzato un nuovo filtro delle comunicazioni. La sezione Filtro dei protocolli potrebbe pertanto risultare non disponibile.

4.1.5.1 SSL

ESET Smart Security 4 permette il controllo di protocolli incapsulati nel protocollo SSL. È possibile utilizzare vari metodi di scansione per le comunicazioni protette SSL che utilizzano certificati attendibili, certificati sconosciuti o certificati esclusi dal controllo delle comunicazioni protette SSL.

Esegui sempre la scansione del protocollo SSL (i certificati esclusi e attendibili restano validi): selezionare questa opzione per controllare tutte le comunicazioni protette SSL ad eccezione di quelle protette da certificati esclusi dal controllo. Se viene stabilita una nuova comunicazione che utilizza un certificato sconosciuto e non firmato, l'utente non verrà avvisato del fatto che tale comunicazione verrà filtrata automaticamente. Quando l'utente accede a un server con un certificato non attendibile contrassegnato come attendibile (aggiunto all'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Chiedi informazioni sui siti non visitati (certificati sconosciuti): Se si accede a un nuovo sito protetto SSL (con un certificato sconosciuto), viene visualizzata una finestra di dialogo in cui è richiesta la scelta di un'azione. In questa modalità è possibile creare un elenco di certificati SSL che verranno esclusi dal controllo.

Non eseguire la scansione del protocollo SSL: se l'opzione è selezionata, il programma non effettuerà scansioni delle comunicazioni SSL.

Se è impossibile verificare la validità del certificato mediante Archivio Autorità di certificazione root attendibili

Informazioni sulla validità del certificato: viene richiesto di selezionare un'azione

Blocca la comunicazione che utilizza il certificato: termina la connessione al sito che utilizza il certificato

nel caso in cui il certificato non sia valido o risulti danneggiato

Informazioni sulla validità del certificato: viene richiesto di selezionare un'azione

Blocca la comunicazione che utilizza il certificato: termina la connessione al sito che utilizza il certificato

4.1.5.1.1 Certificati attendibili

In aggiunta all'Archivio Autorità di certificazione radice attendibili integrato, dove ESET Smart Security 4 memorizza i certificati attendibili, è possibile creare un elenco personalizzato di certificati attendibili visualizzabile in **Configurazione (F5)** > **Filtro protocolli > SSL >**

Certificati attendibili.

4.1.5.1.2 Certificati esclusi

La sezione Certificati esclusi contiene i certificati ritenuti sicuri. Il programma non verificherà il contenuto delle comunicazioni crittografate che utilizzano i certificati presenti nell'elenco. Si consiglia di installare solo i certificati Web di cui è garantita la sicurezza e che non richiedono il filtro del contenuto.

4.1.6 Impostazione parametri motore ThreatSense

ThreatSense è il nome di una tecnologia che consiste in una serie di complessi metodi di rilevamento delle minacce. Questa tecnologia è proattiva, il che significa che fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare la protezione del sistema. Il motore di scansione è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di impostazione della tecnologia ThreatSense consentono all'utente di specificare diversi parametri di scansione:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di disinfezione e così via.

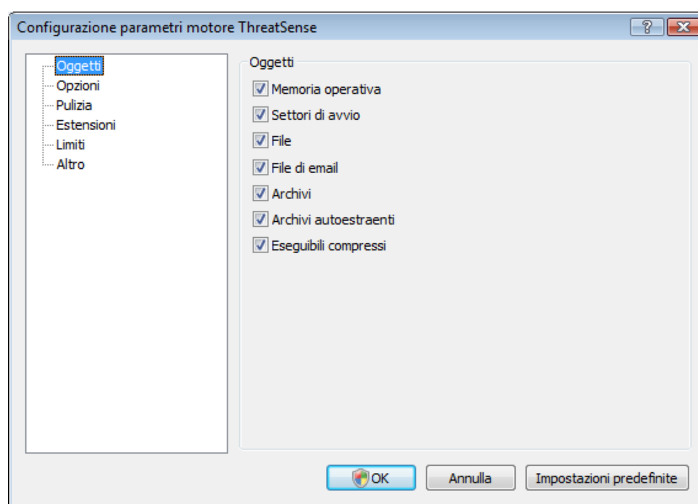
Per aprire la finestra di configurazione, fare clic sul pulsante **Impostazione...** presente in qualsiasi finestra di configurazione del modulo che utilizza la tecnologia ThreatSense (vedere di seguito). Scenari di protezione diversi possono richiedere configurazioni diverse. ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione del file system in tempo reale
- Controllo del file di avvio del sistema
- Protezione email
- Protezione accesso Web
- Controllo computer su richiesta

I parametri di ThreatSense sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire il controllo euristico avanzato nel modulo di protezione del file system in tempo reale potrebbe provocare un rallenatamento del sistema (in genere, con questi metodi vengono controllati solo i file appena creati). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, con l'eccezione di Controllo computer.

4.1.6.1 Configurazione degli oggetti

Nella sezione **Oggetti** è possibile definire i componenti e i file del computer saranno controllati alla ricerca di infiltrazioni.



Memoria operativa: consente di eseguire la scansione per la ricerca di minacce nella memoria operativa del sistema.

Settori di avvio: consente di eseguire il controllo alla ricerca di virus nei settori di avvio

File: consente di eseguire il controllo di tutti i tipi di file più comuni (programmi, immagini, file audio, file video, database e così via)

File di email: consente di eseguire il controllo nei file speciali in cui sono contenuti i messaggi di email

Archivi: consente di eseguire il controllo dei file compressi in archivi (.rar, .zip, .arj, .tar e così via)

Archivi-autoestraenti: consente di eseguire il controllo sui file contenuti in file di archivio-autoestraenti, che in genere si presentano con un'estensione .exe

Eseguibili compressi: i file eseguibili compressi (a differenza dei file di archivio standard) vengono decompressi in memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).

4.1.6.2 Opzioni

Nella sezione Opzioni, l'utente può selezionare i metodi da utilizzare per il controllo del sistema alla ricerca di infiltrazioni. Sono disponibili le seguenti opzioni:

Firme: le firme consentono di rilevare e identificare in modo esatto e affidabile le infiltrazioni in base al relativo nome, utilizzando le firme antivirali.

Euristica: Euristica è un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).

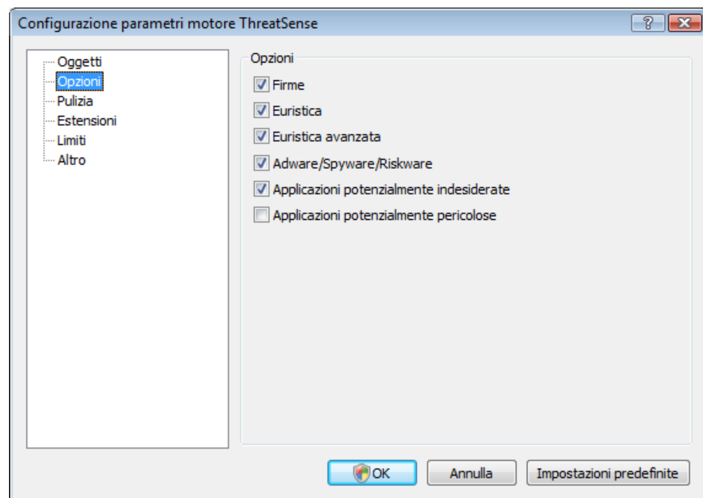
Euristica avanzata: comprende un algoritmo di euristica unico sviluppato da ESET e ottimizzato per il rilevamento di worm e trojan horse scritto in linguaggi di programmazione di alto livello. Grazie alle funzioni di euristica avanzata, la capacità di rilevamento del programma è decisamente maggiore.

Adware/Spyware/Riskware: questa categoria comprende software che raccoglie informazioni riservate sugli utenti senza il loro consenso informato e comprende anche il software che visualizza pubblicità.

Applicazioni potenzialmente pericolose: applicazioni potenzialmente pericolose è la classificazione utilizzata per software commerciale legittimo. Comprende programmi quali strumenti di accesso remoto e, per questo motivo, questa opzione è disattivata in modo predefinito.

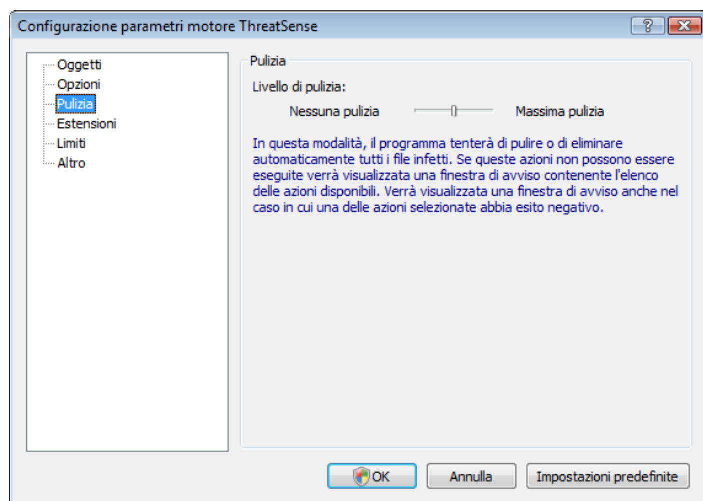
Applicazioni potenzialmente indesiderate: per applicazioni potenzialmente indesiderate non si intendono applicazioni necessariamente dannose, ma in grado di influire sulle prestazioni del computer in modo

negativo. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre pop-up indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.



4.1.6.3 Pulizia

Le impostazioni di disinfezione determinano il comportamento dello scanner durante la disinfezione di file infetti. Sono disponibili 3 livelli di disinfezione:



Nessuna pulitura
I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione.

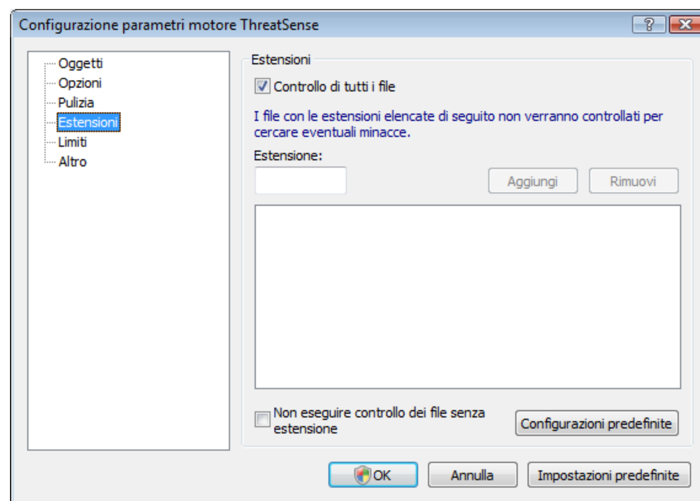
Livello predefinito
Il programma tenterà di pulire o eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni. La scelta tra queste azioni viene visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.

Massima disinfezione
Il programma pulirà o eliminerà tutti i file infetti (inclusi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Se non è possibile eseguire la disinfezione, verrà visualizzata una finestra di allarme in cui l'utente potrà scegliere un'azione da eseguire.

Avvertenza:
Nella modalità predefinita viene eliminato l'intero file di archivio solo se tutti i file che contiene sono infetti. Se contiene anche file non infetti, l'archivio non verrà eliminato. Se viene rilevato un file di archivio infetto nella modalità Massima pulitura, verrà eliminato l'intero file, anche se sono presenti file puliti.

4.1.6.4 Estensioni

Un'estensione è la parte di nome del file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da controllare.



Per impostazione predefinita, tutti i file vengono controllati indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione. Se la casella di controllo **Controllo di tutti i file** è deselezionata, l'elenco viene modificato in modo da visualizzare le estensioni dei file controllati. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire la scansione delle estensioni desiderate.

Per attivare il controllo dei file senza estensione, scegliere l'opzione **Controlla file senza estensione**.

L'esclusione di file dal controllo è utile nel caso in cui il controllo di determinati tipi di file causi operazioni non corrette nel programma che utilizza le estensioni. Ad esempio, è consigliabile escludere le estensioni .edb, .eml e .tmp durante l'utilizzo di MS Exchange Server.

4.1.6.5 Limiti

La sezione Limiti consente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire la scansione:

Dimensioni massime oggetti (byte)
Determina la dimensione massima degli oggetti su cui eseguire la scansione. Il modulo antivirus eseguirà unicamente la scansione degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare il valore predefinito, poiché non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dalla scansione.

Durata massima scansione dell'oggetto (sec.)
Definisce il valore massimo di tempo destinato alla scansione di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà la scansione dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che la scansione sia stata completata.

Livello di nidificazione degli archivi
Specifica il livello massimo di scansione degli archivi. Si consiglia di non modificare il valore predefinito di 10; in circostanze normali non sussiste alcun motivo per farlo. Se la scansione termina prima del tempo a causa del numero di archivi nidificati, l'archivio non verrà controllato.

Dimensioni massime dei file in archivio (byte)
Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno controllati. Se per questo motivo la scansione termina prima del tempo, l'archivio non verrà controllato.

4.1.6.6 Altro

Scansione flussi di dati alternativi (ADS)
I flussi di dati alternativi (ADS) utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle tecniche di scansione standard. Molte infiltrazioni cercano di non essere rilevate presentandosi come flussi di dati alternativi.

Esegui scansioni in background con priorità bassa
Ogni sequenza di scansione utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare la scansione in background con priorità bassa e risparmiare risorse per le applicazioni.

Registra tutti gli oggetti
Se questa opzione è selezionata, il file di rapporto riporta tutti i file controllati, anche quelli non infetti.

Mantieni indicatore data e ora dell'ultimo accesso
Selezionare questa opzione per mantenere la data e l'ora di accesso originali ai file su cui è stata eseguita la scansione anziché aggiornarli (ad esempio, per l'utilizzo di sistemi di backup dei dati).

Scorri registro
Questa opzione consente di abilitare/disabilitare lo scorrimento del rapporto. Se viene selezionata, è possibile scorrere le informazioni verso l'alto nella finestra di visualizzazione.

Visualizza notifica sul completamento della scansione in una finestra separata
Consente di aprire una finestra indipendente che contiene informazioni sui risultati della scansione.

4.1.7 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi: pagine Web, cartelle condivise, messaggi e-mail o periferiche rimovibili (USB, dischi esterni, CD, DVD, dischetti, e così via).

Se il computer mostra segnali di infezione da malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile seguire le seguenti istruzioni:

- Avviare ESET Smart Security e scegliere **Computer scan**
- Scegliere **Controllo standard**
  (per ulteriori informazioni, vedere Controllo standard).
- Al termine della scansione, controllare nel rapporto il numero di file sottoposti a scansione, file infetti e file puliti.

Se si desidera effettuare il controllo solo di una parte del disco, scegliere **Controllo personalizzato** e selezionare le destinazioni da controllare alla ricerca di virus.

Per un esempio di come ESET Smart Security gestisca le infiltrazioni, si supponga che il monitor del file system in tempo reale, che utilizza il livello di disinfezione predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite nel modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni in genere disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, perché con tale opzione si lasciano i file infetti inalterati. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

Disinfezione ed eliminazione
Applicare la disinfezione nel caso in cui un file pulito sia stato attaccato da un virus che ha aggiunto al file pulito del codice dannoso. In tal caso, prima tentare di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente di codice dannoso, verrà eliminato.



Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (in genere dopo il riavvio del sistema).

Eliminazione dei file negli archivi
In modalità di pulizia predefinita, l'intero archivio viene eliminato solo quando contiene tutti file infetti, senza alcun file pulito. In pratica gli archivi non vengono eliminati quando contengono anche file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di un controllo di tipo Massima pulitura, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

4.2 Personal firewall

Il Personal firewall controlla tutto il traffico di rete in entrata e in uscita dal sistema, consentendo o rifiutando singole connessioni di rete in base a specifiche regole di filtro. Offre protezione contro gli attacchi da computer remoti e consente di bloccare alcuni servizi. Offre inoltre protezione antivirus per i protocolli HTTP e POP3. Questa funzionalità rappresenta un elemento molto importante nella protezione del computer.

4.2.1 Modalità di filtro

Sono disponibili tre modalità di filtro per ESET Smart Security – Firewall. Il comportamento del firewall cambia in base alla modalità selezionata. Le modalità di filtro influenzano inoltre il livello richiesto di interazione dell'utente.

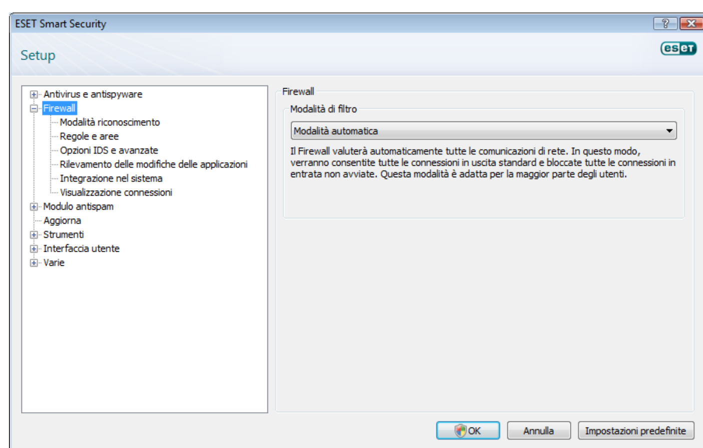
Il filtro può essere eseguito in una delle cinque modalità seguenti:

- La modalità di filtro automatico è quella predefinita. È adatta agli utenti che preferiscono un utilizzo semplice e comodo del firewall, senza dover definire delle regole. Questa modalità consente tutto il traffico in uscita per il sistema e blocca tutte le nuove connessioni avviate sul lato rete.
- Modalità automatica con eccezioni (regole definite dall'utente) La modalità automatica consente inoltre di aggiungere regole personalizzate.

- La modalità di filtro interattivo consente di creare una configurazione personalizzata per il firewall. Quando viene rilevata una comunicazione e non esiste alcuna regola applicabile, viene visualizzata una finestra di dialogo che segnala una connessione sconosciuta. La finestra di dialogo consente di accettare o rifiutare la comunicazione e la decisione può essere ricordata come nuova regola del Personal firewall. Se l'utente decide di creare una nuova regola, tutte le connessioni future di questo tipo saranno consentite o bloccate in base a questa regola.

- La modalità basata su criteri blocca tutte le connessioni non definite da una regola specifica che le consente. Questa modalità consente agli utenti esperti di definire regole che permettano solo connessioni sicure e desiderate. Tutte le altre connessioni non specificate saranno bloccate dal Personal firewall.

- La modalità riconoscimento crea e salva automaticamente le regole, inoltre, è ideale per la configurazione iniziale del firewall. Non è richiesta alcuna interazione utente, poiché ESET Smart Security esegue il salvataggio seguendo parametri predefiniti. Modalità riconoscimento non è una modalità protetta, pertanto è consigliabile utilizzarla solo fintanto che non si siano create tutte le regole richieste per le comunicazioni.



4.2.2 Blocca tutto il traffico di rete: disconnessione rete

L'unica opzione disponibile per bloccare in modo completo tutto il traffico di rete è l'opzione **Blocca tutto il traffico di rete: disconnessione rete**. Le eventuali comunicazioni in entrata e in uscita vengono bloccate dal Personal firewall senza che venga visualizzato alcun messaggio di avviso. Utilizzare questa opzione di blocco solo se si sospettano rischi di protezione critici che richiedono la disconnessione del sistema dalla rete.



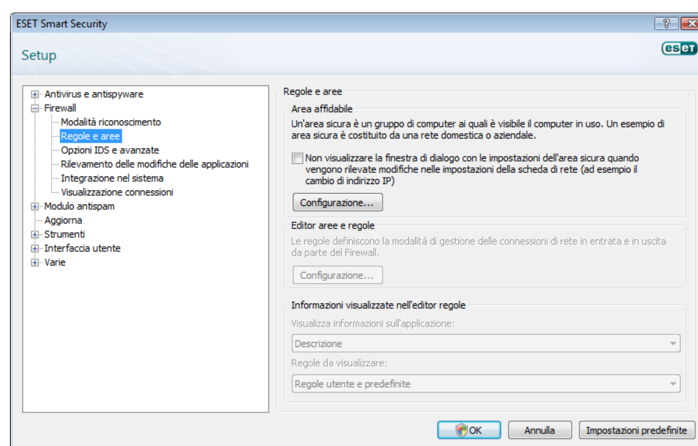
4.2.3 Filtro disattivato: consenti tutto il traffico

L'opzione relativa alla disattivazione del filtro consente una configurazione opposta rispetto al blocco di tutte le comunicazioni illustrato in precedenza. Se selezionata, tutte le opzioni di filtro del Personal firewall saranno disattivate e saranno consentite tutte le connessioni in ingresso e in uscita. In presenza di una rete, l'effetto è pari alla mancanza assoluta di un firewall.

4.2.4 Configurazione e uso delle regole

Le regole rappresentano un insieme di condizioni utilizzate per verificare tutte le connessioni di rete e tutte le azioni assegnate a queste condizioni. Nel caso in cui sia stabilita una connessione definita da una regola, nel firewall è possibile stabilire l'azione da eseguire.

Per accedere all'impostazione di filtro della regola, selezionare **Impostazione avanzata (F5) > Personal firewall > Regole e aree**. Per visualizzare la configurazione corrente, scegliere **Configurazione** nella sezione **Editor aree e regole** (se il Personal firewall è impostato sulla **modalità di filtro automatico**, queste impostazioni non sono disponibili).



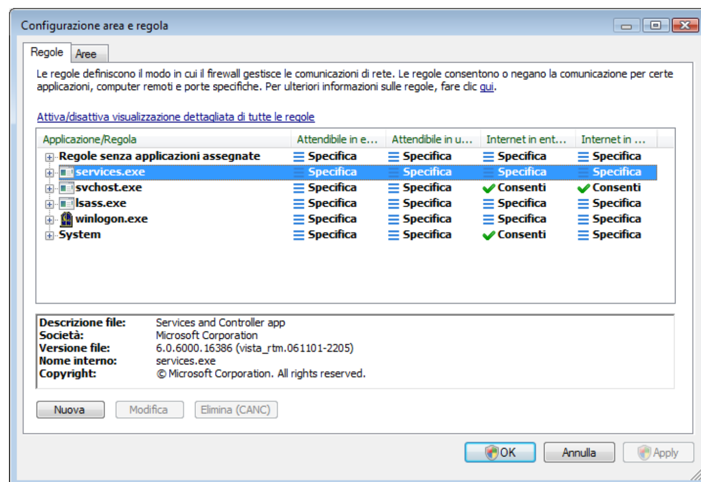
Nella finestra **Configurazione area e regola** viene visualizzata una panoramica delle regole o aree (in base alla scheda selezionata). La finestra è suddivisa in due sezioni. Nella sezione superiore è visualizzato un elenco sintetico di tutte le regole. Nella sezione inferiore sono visualizzati dettagli sulla regola selezionata nella sezione superiore. Nella parte inferiore della finestra, i pulsanti **Nuova**, **Modifica** ed **Elimina** consentono di configurare le regole.

In relazione alla direzione delle comunicazioni, le connessioni possono essere suddivise in connessioni in entrata e in uscita. Le connessioni in entrata vengono avviate da un computer remoto che tenta di stabilire la connessione con il sistema locale. Le connessioni in uscita funzionano in senso opposto: il lato locale tenta di stabilire la connessione con un computer remoto.

Quando viene rilevata una nuova comunicazione sconosciuta, è necessario considerare con attenzione se accettarla o rifiutarla. Le connessioni non desiderate, non sicure o completamente sconosciute costituiscono un rischio per la protezione del sistema. Se si stabilisce una connessione di questo tipo, è opportuno prestare particolare attenzione al lato remoto e all'applicazione che tenta di connettersi al computer. Molte infiltrazioni cercano di ottenere e inviare dati privati o scaricare altre applicazioni dannose sulle workstation host. Il Personal firewall consente di rilevare e interrompere queste connessioni.

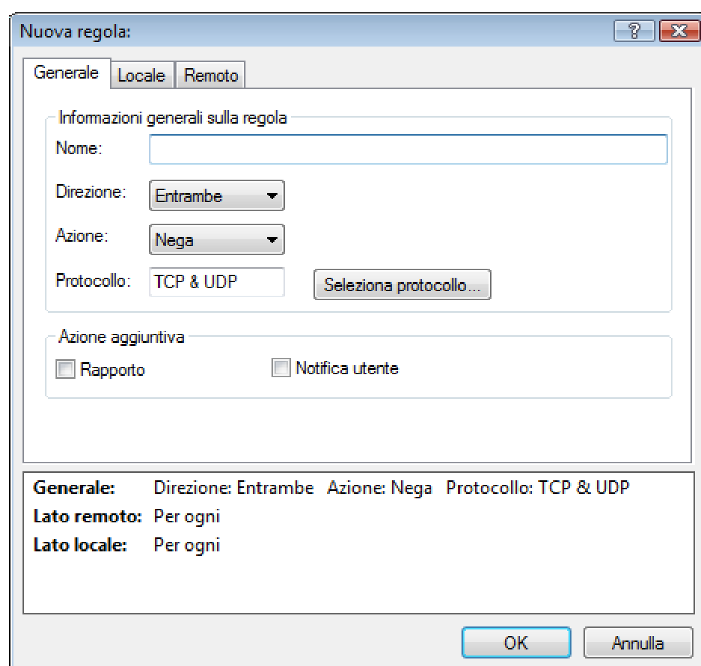
4.2.4.1 Creazione di nuove regole

Durante l'installazione di una nuova applicazione con accesso alla rete o in caso di modifica di una connessione esistente (lato remoto, numero di porta e così via), è necessario creare una nuova regola.



Per aggiungere una nuova regola, verificare che sia selezionata la scheda **Regole**. Fare clic sul pulsante **Nuova** nella finestra **Configurazione area e regola**. Se si fa clic su questo pulsante viene visualizzata una nuova finestra di dialogo che consente di specificare una nuova regola. La parte superiore della finestra contiene tre schede:

- Generale: consente di specificare il nome della regola, la direzione, l'azione e il protocollo. La direzione può essere in entrata o in uscita (o entrambi). Per azione si intende consentire o rifiutare la connessione specificata.
- Locale: consente di visualizzare le informazioni sul lato locale della connessione, tra cui il numero della porta locale o l'intervallo di porte e il nome dell'applicazione in comunicazione.
- Remoto: questa scheda contiene informazioni sulle porte remote (intervallo porte). Consente inoltre all'utente di definire un elenco di indirizzi IP remoti o aree per una specifica regola.



Un esempio di creazione di una nuova regola consiste nel consentire al browser di accedere alla rete. In questo caso è consigliabile attenersi alla seguente procedura:

- Nella scheda **Generale**, attivare le comunicazioni in uscita mediante il protocollo TCP & UDP
- Aggiungere il processo che rappresenta l'applicazione browser (per Internet Explorer è iexplore.exe) nella scheda **Locale**
- Nella scheda **Remoto** attivare il numero di porta 80 solo se si desidera consentire esclusivamente servizi World Wide Web standard

4.2.4.2 Modifica delle regole

Per modificare una regola esistente, fare clic sul pulsante **Modifica**. È possibile modificare tutti i parametri indicati in precedenza (descritti nel capitolo "Creazione di nuove regole").

La modifica è necessaria ogni volta che uno dei parametri controllati viene cambiato. Di conseguenza, la regola non soddisfa le condizioni e non è possibile applicare l'azione specificata. Alla fine, la connessione può essere rifiutata il che può causare problemi con il funzionamento dell'applicazione in questione. Un esempio è la modifica di un indirizzo di rete o di un numero di porta per il lato remoto.

4.2.5 Configurazione aree

Le aree rappresentano gruppi di indirizzi di rete che creano un gruppo logico unico. A ciascun indirizzo del gruppo specificato vengono assegnate regole simili, definite in modo centralizzato per l'intero gruppo. Un esempio di gruppo di questo tipo è costituito dall'Area sicura. L'area sicura rappresenta un gruppo di indirizzi di rete considerati completamente affidabili dall'utente e che non vengono in alcun modo bloccati dal Personal firewall.

È possibile configurare queste aree mediante la scheda **Aree** nella finestra **Configurazione area e regola**, utilizzando il pulsante **Nuovo**. Nella finestra visualizzata immettere il nome dell'area, la descrizione e l'elenco degli indirizzi di rete.

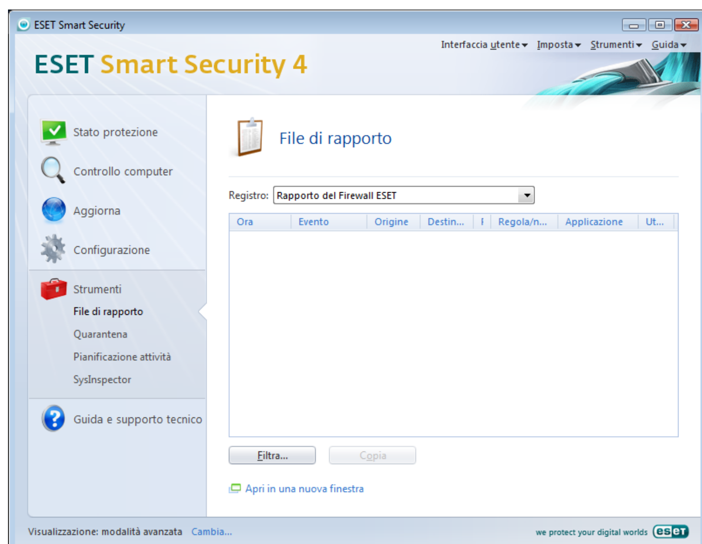
4.2.6 Stabilire la connessione: rilevamento

Il Personal firewall rileva tutte le connessioni di rete non appena queste vengono create. La modalità firewall attiva (automatica, interattiva o basata su criteri) determina le azioni eseguite per la nuova regola. Se è attivata la modalità automatica o basata su criteri, il Personal firewall eseguirà delle azioni predefinite senza l'intervento dell'utente. In modalità interattiva viene invece visualizzata una finestra informativa che riporta il rilevamento di una nuova connessione di rete, con informazioni dettagliate sulla connessione. L'utente può scegliere se consentire la connessione o rifiutarla (bloccarla). Se è necessario consentire ripetutamente la stessa connessione nella finestra di dialogo, è consigliabile creare una nuova regola per la connessione. A tal fine, selezionare l'opzione **Ricorda azione (crea regola)** e salvare l'azione come nuova regola per il Personal firewall. Se il firewall riconoscerà la stessa connessione in futuro, applicherà la regola esistente.



È necessario prestare particolare attenzione quando si creano nuove regole. Se si consentono tutte le connessioni, il Personal firewall non potrà svolgere la funzione per la quale è stato installato. Sono riportati di seguito importanti parametri per le connessioni:

- **Lato remoto:** consentire la connessione solo a indirizzi affidabili e noti
- **Applicazione locale:** non è consigliabile consentire la connessione di applicazioni e processi sconosciuti
- **Numero di porta:** La comunicazione sulle porte normali (ad esempio per il Web, numero di porta 80) è in genere sicura



Per diffondersi, le infiltrazioni utilizzano spesso la connessione a Internet e connessioni nascoste per infettare sistemi remoti. Se le regole sono configurate correttamente, un Personal firewall diventa un utile strumento per la protezione contro molti attacchi di malware.

4.2.7 Registrazione

ESET Smart Security - Firewall salva gli eventi importanti in un file di rapporto, che può essere visualizzato direttamente dal menu principale del programma. Scegliere **Strumenti > File di rapporto**, quindi selezionare **Rapporto del firewall ESET** dal menu a discesa **Registro**.

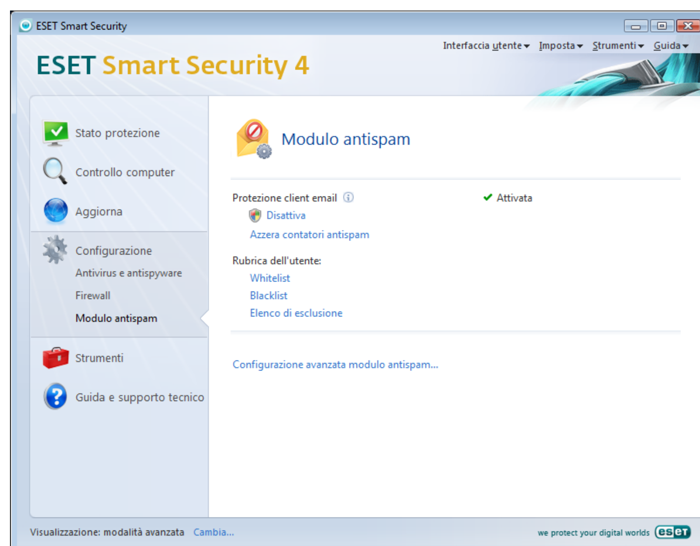
I file di rapporto sono uno strumento importantissimo per il l'analisi di errori e per rivelare intrusioni nel sistema ed è opportuno prestarvi l'attenzione appropriata. I rapporti di Firewall ESET contengono i seguenti dati:

- Data e ora dell'evento
- Nome dell'evento
- Indirizzo di rete di origine e di destinazione
- Protocollo di comunicazione di rete
- Regola applicata o nome del worm, se identificato
- Applicazione coinvolta

Un'attenta analisi di questi dati può essere d'aiuto per rilevare i tentativi di compromettere la protezione del sistema. Molti altri fattori indicano potenziali rischi per la protezione e consentono all'utente di ridurre al minimo il loro impatto: connessioni troppo frequenti da posizioni sconosciute, tentativi ripetuti di stabilire connessioni, comunicazione da parte di applicazioni sconosciute o utilizzo di numeri di porta insoliti.

4.3 Protezione antispam

Attualmente i messaggi e-mail non desiderati: definiti spam: costituiscono uno dei maggiori problemi delle comunicazioni elettroniche. Rappresentano infatti quasi l'80% di tutte le comunicazioni e-mail. La protezione antispam consente di proteggersi da questo problema. Grazie alla combinazione di una serie di principi molto efficaci, il modulo antispam fornisce un filtro superiore.



Un principio essenziale per il rilevamento dello spam è la capacità di riconoscere messaggi indesiderati in base a indirizzi affidabili predefiniti (whitelist) e agli indirizzi di spam (blacklist). Tutti gli indirizzi del client e-mail vengono aggiunti automaticamente alla whitelist, oltre a tutti gli altri indirizzi contrassegnati dall'utente come sicuri.

Il metodo principale per rilevare lo spam è la scansione delle proprietà di un messaggio e-mail. I messaggi ricevuti vengono controllati in base ai criteri antispam di base (definizioni di messaggi, euristica statistica, riconoscimento di algoritmi e altri metodi univoci) e dal valore di indice risultante è possibile determinare se un messaggio è spam o meno.

Anche il filtro Bayes viene utilizzato per il filtro. Contrassegnando i messaggi come *spam* e *non spam*, l'utente crea un database di parole utilizzate in ciascuna di tali categorie. Più completo è il database, maggiore sarà la precisione dei risultati.

Una combinazione dei metodi illustrati garantisce un'elevata percentuale di rilevamento di spam.

ESET Smart Security supporta la protezione antispam per Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla

Thunderbird.

4.3.1 Riconoscimento automatico antispam

Il riconoscimento automatico antispam è collegato al filtro Bayes, cui si è accennato in precedenza. L'importanza delle singole parole cambia durante il processo di "riconoscimento" per contrassegnare i singoli messaggi come spam o non spam. Di conseguenza, man mano che aumenta il numero di messaggi classificati (contrassegnati come spam o non spam), migliorerà anche l'accuratezza dei risultati ottenuti con il filtro Bayes.

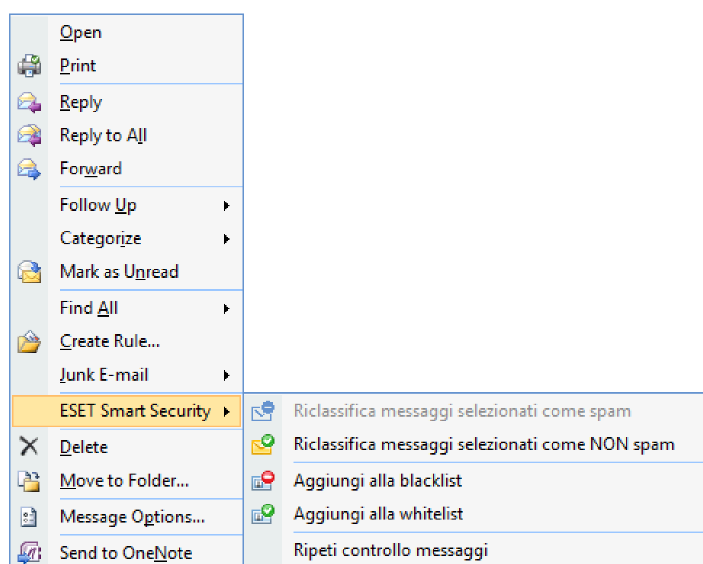
Aggiungere gli indirizzi noti alla whitelist per escludere dal filtro i messaggi provenienti da questi indirizzi.

4.3.1.1 Aggiunta di indirizzi alla whitelist

Gli indirizzi email che appartengono a persone con cui l'utente comunica spesso possono essere aggiunti all'elenco di indirizzi "sicuri", definito whitelist. In questo modo si è certi che nessun messaggio proveniente da un indirizzo della whitelist verrà mai classificato come spam. Per aggiungere un nuovo indirizzo alla whitelist, fare clic con il pulsante destro del mouse sul messaggio email desiderato e selezionare **Aggiungi alla whitelist** nell'opzione del menu di scelta rapida ESET Smart Security oppure selezionare **Indirizzo affidabile** nella barra degli strumenti Antispam di ESET Smart Security nella parte superiore della finestra del client email. La procedura è identica per gli indirizzi spam. Se un indirizzo email viene inserito nella blacklist, tutti i messaggi email inviati da tale indirizzo saranno classificati come spam.

4.3.1.2 Contrassegnare messaggi come spam

Qualsiasi messaggio visualizzato nel client e-mail può essere contrassegnato come spam. A tal fine, utilizzare il menu di scelta rapida (fare clic con il pulsante destro del mouse su **ESET Smart Security > Riclassifica messaggi selezionati come spam**) oppure scegliere l'opzione **Spam** dalla barra degli strumenti Antispam di ESET Smart Security nel client email.



I messaggi riclassificati vengono spostati automaticamente nella cartella SPAM, ma l'indirizzo e-mail del mittente non viene aggiunto alla blacklist. Allo stesso modo, i messaggi possono essere classificati come "non spam". Se vengono classificati come non spam, i messaggi della cartella della **posta indesiderata verranno spostati nella relativa cartella** originale. Se un messaggio viene contrassegnato come non spam, l'indirizzo del mittente non viene automaticamente aggiunto alla whitelist.

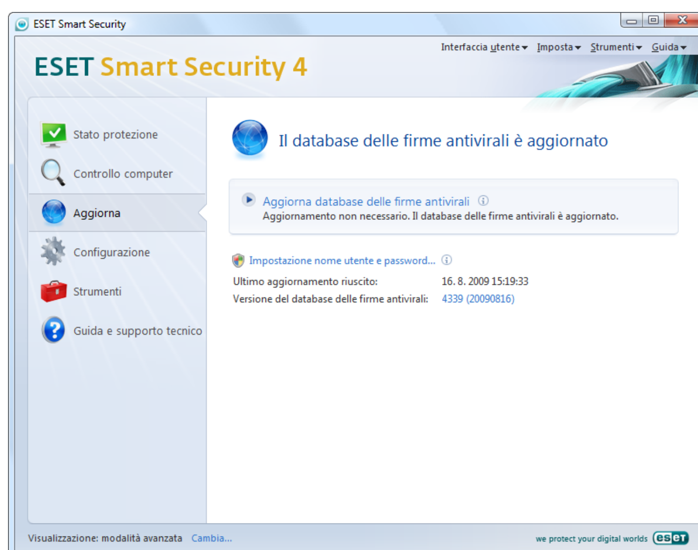
4.4 Aggiornamento del programma

L'aggiornamento periodico del sistema rappresenta un punto fondamentale per ottenere il massimo livello di protezione garantito da ESET Smart Security. Il Modulo di aggiornamento assicura che il programma sia sempre aggiornato. Questo risultato si ottiene in due modi: aggiornando il database di firme antivirali e aggiornando tutti i componenti del sistema.

È possibile visualizzare alcune informazioni sullo stato corrente degli aggiornamenti facendo clic su **Aggiorna**, tra cui la versione del database delle firme antivirali e l'eventuale necessità di un aggiornamento. Sono inoltre disponibili l'opzione che consente di attivare il processo di aggiornamento immediatamente, **Aggiorna database delle firme antivirali**, e le opzioni per la configurazione dell'aggiornamento di base, come il nome utente e la password per i server di aggiornamento di ESET.

La finestra delle informazioni contiene anche ulteriori dettagli, quali la data e l'ora dell'ultimo aggiornamento eseguito correttamente e il numero del database di firme antivirali. Questa indicazione numerica è un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

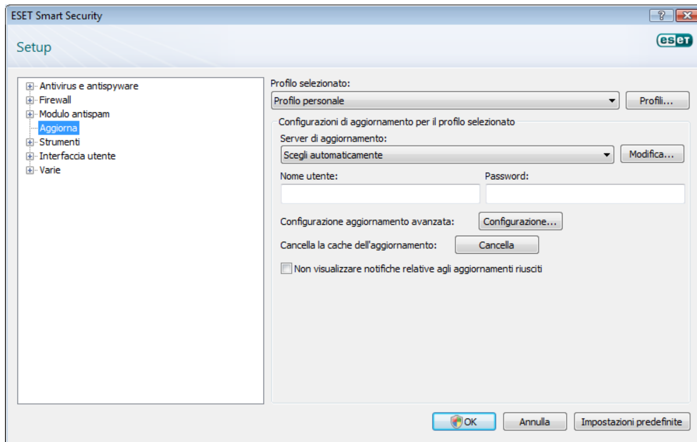
Utilizzare il collegamento **Registra** per aprire il modulo di registrazione che consentirà la registrazione della nuova licenza in ESET. I dati di autenticazione verranno quindi recapitati via e-mail.



NOTA: il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET Smart Security.

4.4.1 Configurazione dell'aggiornamento

La sezione Configurazione aggiornamento consente di specificare informazioni sull'origine dell'aggiornamento, come i server di aggiornamento e i dati per l'autenticazione presso tali server. Per impostazione predefinita, il campo **Server di aggiornamento:** è impostato su **Scegli automaticamente**. Questo valore garantisce che i file di aggiornamento vengano scaricati automaticamente dal server ESET con meno traffico di rete. Le opzioni di configurazione dell'aggiornamento sono disponibili nella struttura Configurazione avanzata (F5), sotto **Aggiorna**.



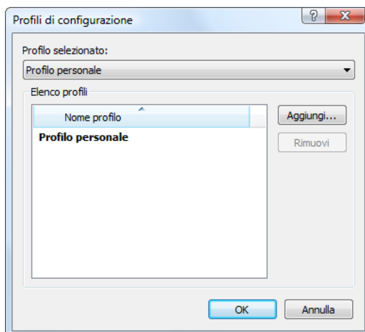
L'elenco di server di aggiornamento esistenti è accessibile tramite il menu a discesa in **Server di aggiornamento.** Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Impostazioni di aggiornamento per il profilo selezionato** e quindi fare clic sul pulsante **Aggiungi**.

L'autenticazione per i server di aggiornamento è garantita da **Nome utente** e **Password** che vengono generati e inviati all'utente da ESET dopo l'acquisto della licenza del prodotto.

4.4.1.1 Profili di aggiornamento

Per diverse configurazioni di aggiornamento, è possibile creare profili di aggiornamento definiti dall'utente, da utilizzare per determinate attività di aggiornamento. La creazione di diversi profili di aggiornamento è particolarmente utile per gli utenti mobili, perché le proprietà di connessione a Internet cambiano regolarmente. Se si modifica l'attività di aggiornamento, gli utenti mobili possono specificare che, quando non è possibile aggiornare il programma utilizzando la configurazione specificata in **Profilo personale**, l'aggiornamento deve essere eseguito utilizzando un profilo alternativo.

Nel menu a discesa **Profilo selezionato** viene visualizzato il profilo selezionato. Nell'impostazione predefinita, questa opzione è impostata su **Profilo personale**. Per creare un nuovo profilo, fare clic sul pulsante **Profili**, quindi sul pulsante **Aggiungi** e immettere il proprio **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da un profilo esistente selezionandolo dal menu a discesa **Copia impostazioni da profilo**.



Durante l'impostazione del profilo è possibile specificare il server di aggiornamento al quale il programma si connetterà e dal quale scaricherà gli aggiornamenti; è possibile utilizzare qualsiasi server dell'elenco di server disponibili, oppure è possibile aggiungere un nuovo server. L'elenco dei server di aggiornamento esistenti è accessibile tramite il menu a discesa in **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, scegliere **Modifica** nella sezione **Configurazioni di aggiornamento per il profilo selezionato** e fare clic sul pulsante **Aggiungi**.

4.4.1.2 Configurazione avanzata dell'aggiornamento

Per visualizzare **Configurazione aggiornamento avanzata**, fare clic sul pulsante **Configurazione**. Nella configurazione aggiornamento avanzata è possibile impostare **Modalità di aggiornamento, Proxy HTTP, LAN** e **Mirror**.

4.4.1.2.1 Modalità di aggiornamento

Nella scheda **Modalità di aggiornamento** sono disponibili opzioni correlate all'aggiornamento dei componenti del programma.

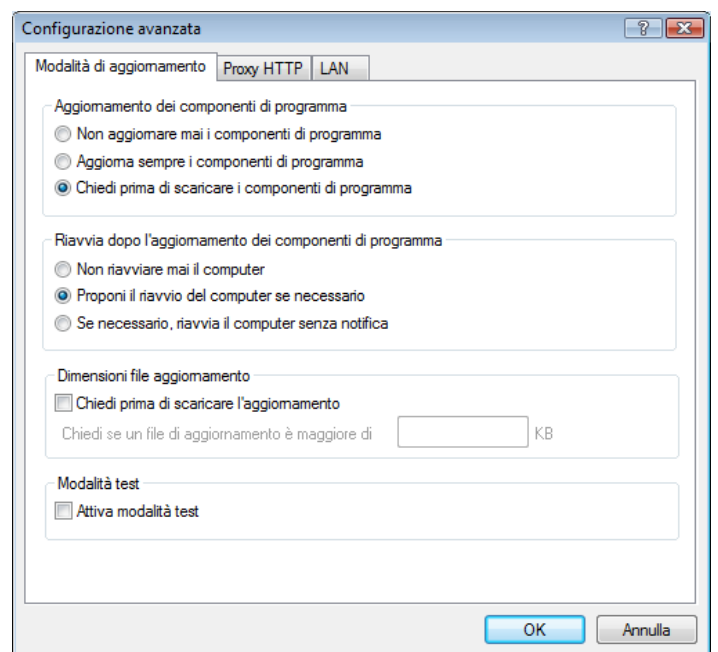
Nella sezione **Aggiornamenti automatici dei componenti di programma** sono disponibili tre opzioni:

- **Non aggiornare mai i componenti di programma**
- **Aggiorna sempre i componenti di programma**
- **Chiedi prima di scaricare i componenti di programma**

La selezione dell'opzione **Non aggiornare mai i componenti di programma** assicura che non venga scaricato un nuovo aggiornamento dei componenti di programma rilasciato da ESET e che non venga eseguito alcun aggiornamento dei componenti di programma sulla workstation specificata. La selezione dell'opzione **Aggiorna sempre i componenti di programma** implica che gli aggiornamenti dei componenti di programma verranno eseguiti ogni volta che sui server di aggiornamento ESET è disponibile un nuovo aggiornamento e che i componenti di programma verranno aggiornati alla versione scaricata.

La selezione della terza opzione, **Chiedi prima di scaricare i componenti di programma**, garantisce che nel programma verrà visualizzato un messaggio con cui si chiede all'utente di confermare il download degli aggiornamenti dei componenti di programma, quando questi saranno disponibili. In tal caso, verrà visualizzata una finestra di dialogo contenente informazioni sugli aggiornamenti dei componenti di programma disponibili e le opzioni che consentono di scegliere se consentire il download o rifiutarlo. In caso di conferma, gli aggiornamenti verranno scaricati e verranno installati i nuovi componenti di programma.

L'opzione predefinita per l'aggiornamento dei componenti di programma è **Chiedi prima di scaricare i componenti di programma**.



Una volta installato un aggiornamento dei componenti di programma, è necessario riavviare il sistema in modo da garantire il corretto funzionamento di tutti i moduli. La sezione **Riavvia dopo l'aggiornamento dei componenti di programma** consente

di selezionare una delle tre opzioni seguenti:

- **Non riavviare mai il computer**
- **Proponi il riavvio del computer se necessario**
- **Se necessario, riavvia il computer senza notifica**

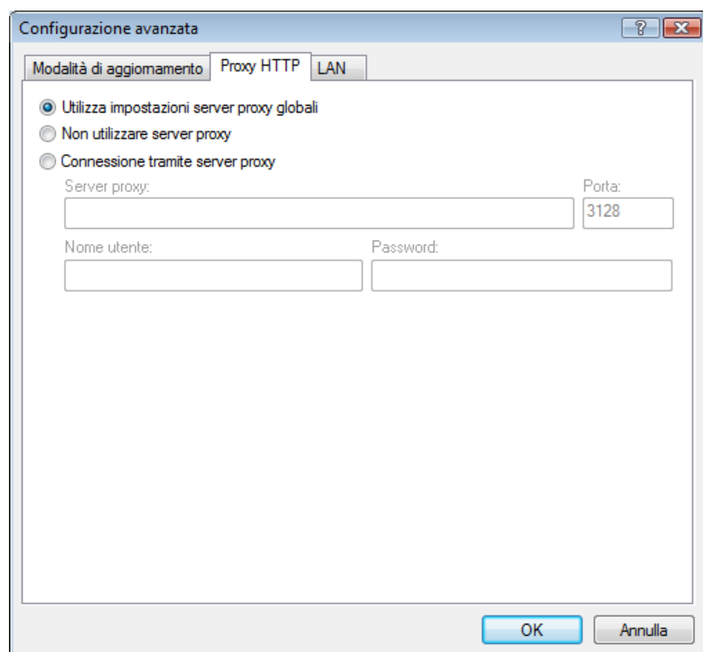
L'opzione predefinita per il riavvio è **Proponi il riavvio del computer se necessario**. La selezione delle opzioni più appropriate per gli aggiornamenti dei componenti di programma all'interno della scheda **Modalità di aggiornamento** dipende dalla workstation in uso. Esistono alcune differenze tra le workstation e i server. Il riavvio automatico del server dopo un aggiornamento di un componente di programma potrebbe, ad esempio, causare gravi danni al sistema.

4.4.1.2.2 Server proxy

Per accedere alle opzioni di configurazione del server proxy per un determinato profilo di aggiornamento: fare clic su **Aggiorna** nella sezione Configurazione avanzata (F5), quindi fare clic sul pulsante **Configurazione** alla destra di **Configurazione aggiornamento avanzata**. Scegliere la scheda **Proxy HTTP** e selezionare una delle tre opzioni seguenti:

- **Utilizza impostazioni server proxy globali**
- **Non utilizzare server proxy**
- **Connessione tramite server proxy** (connessione definita dalle proprietà della connessione)

La selezione dell'opzione **Utilizza impostazioni server proxy globali** consente di utilizzare le opzioni di configurazione del server proxy già specificate in **Varie > Server proxy** nella struttura di configurazione avanzata.



Selezionare l'opzione **Non utilizzare server proxy** per definire in modo esplicito che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET Smart Security.

Selezionare l'opzione **Connessione tramite server proxy** se per l'aggiornamento di ESET Smart Security si desidera utilizzare un server proxy diverso dal server proxy specificato nelle impostazioni globali (**Varie > Server Proxy**). In tal caso, sarà necessario specificare delle informazioni aggiuntive: l'indirizzo del **server proxy**, la **porta** di comunicazione e il **nome utente** e la **password** per il server proxy, se necessario.

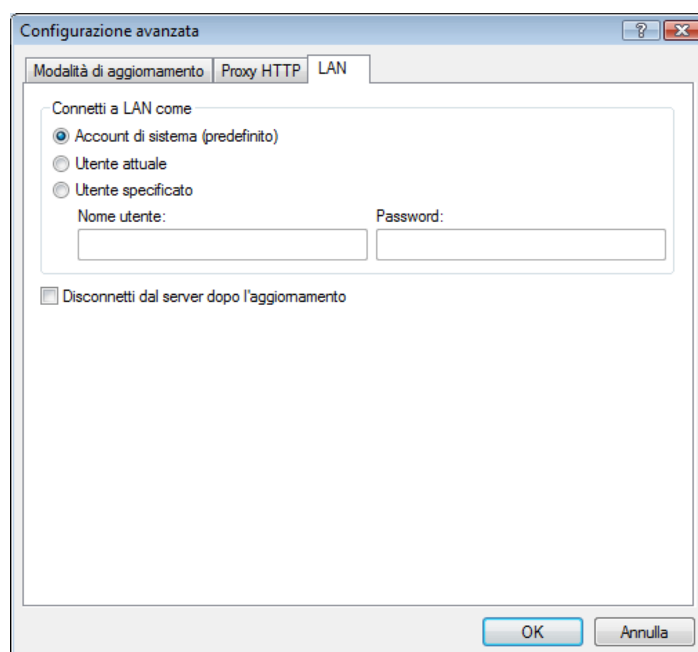
Questa opzione deve essere inoltre selezionata quando le impostazioni del server proxy non sono state impostate globalmente, ma ESET Smart Security utilizzerà per gli aggiornamenti la connessione tramite un server proxy.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

4.4.1.2.3 Connessione alla LAN

Durante l'aggiornamento da un server locale con un sistema operativo basato su NT, in modo predefinito è richiesta l'autenticazione per ciascuna connessione di rete. Nella maggior parte dei casi, un account di sistema locale non dispone di diritti di accesso sufficienti per la cartella Mirror (che contiene le copie dei file di aggiornamento). In questo caso, immettere nome utente e password nella sezione di configurazione dell'aggiornamento o specificare un account esistente che il programma utilizzerà per il server di aggiornamento (Mirror).

Per configurare un account di questo tipo, fare clic sulla scheda **LAN**. Nella sezione **Connetti a LAN come** sono disponibili le opzioni **Account di sistema (predefinito)**, **Utente attuale** e **Utente specificato**.



Selezionare l'opzione **Account di sistema** per utilizzare l'account di sistema per l'autenticazione. In genere se nella sezione principale di configurazione dell'aggiornamento non sono specificati dati di autenticazione, non viene eseguito alcun processo di autenticazione.

Per accertarsi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito l'accesso, selezionare **Utente attuale**. Lo svantaggio di questa soluzione è che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito correntemente l'accesso.

Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione.

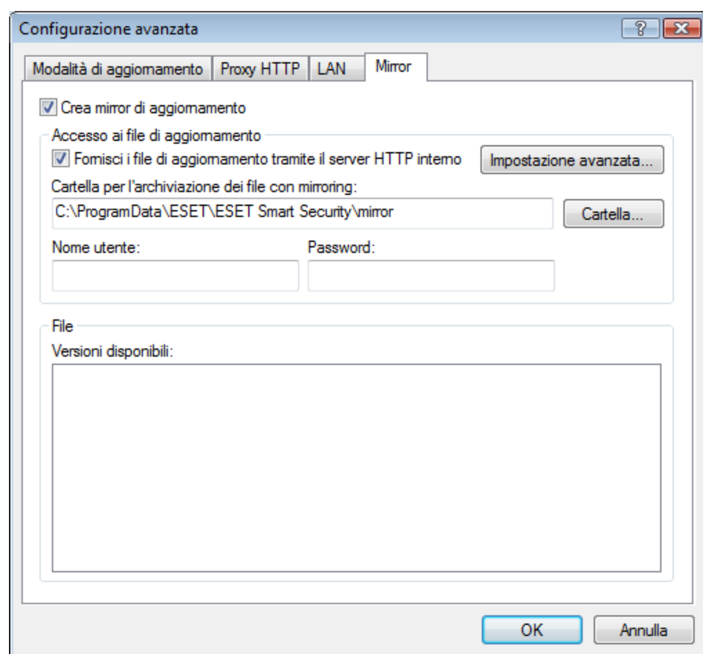
L'opzione predefinita per la connessione alla LAN è **Account di sistema**.

Avvertenza:
Se è attivata l'opzione **Utente attuale** o l'opzione **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. Per questo motivo è consigliabile inserire i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di configurazione dell'aggiornamento, i dati di autenticazione vanno immessi come segue: nome_dominio\utente (se si tratta di un gruppo di lavoro, immettere nome_gruppodilavoro\nome) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

4.4.1.2.4 Creazione di copie di aggiornamento: Mirror

ESET Smart Security Business Edition consente all'utente di creare copie di file di aggiornamento che è possibile utilizzare per aggiornare altre workstation della rete. L'aggiornamento delle workstation client da un Mirror consente di ottimizzare il bilanciamento del carico di rete e di risparmiare banda per la connessione a Internet.

Le opzioni di configurazione per il Mirror del server locale sono disponibili (dopo aver aggiunto una chiave di licenza valida nella gestione delle licenze, che si trova nella sezione di configurazione avanzata di ESET Smart Security Business Edition) nella sezione **Configurazione aggiornamento avanzata** (per accedere a questa sezione, premere F5 e fare clic su **Aggiorna** nella struttura Configurazione avanzata. Fare clic sul pulsante **Configurazione** accanto a **Configurazione aggiornamento avanzata**, quindi selezionare la scheda **Mirror**).



La prima operazione da eseguire per configurare il Mirror consiste nel selezionare la casella di controllo **Crea mirror di aggiornamento**. Quando si seleziona questa opzione vengono attivate altre opzioni di configurazione del Mirror, come la modalità di accesso ai file di aggiornamento e il percorso di aggiornamento per i file del mirror.

I metodi di attivazione del mirror sono descritti in dettaglio nel capitolo successivo "Varianti di accesso al mirror". Per ora basta notare che sono disponibili due varianti di base per l'accesso al Mirror: la cartella con i file di aggiornamento può essere presentata come Mirror come cartella di rete condivisa o come Mirror come server HTTP.

La cartella dedicata alla memorizzazione dei file di aggiornamento per il Mirror è definita nella sezione **Cartella per l'archiviazione dei file del morror**. Fare clic su **Cartella...** per cercare la cartella desiderata sul computer locale o sulla cartella di rete condivisa. Se è necessaria l'autorizzazione per la cartella specificata, i dati di autenticazione devono essere specificati nei campi **Nome utente** e **Password**. Nome utente e Password devono essere specificati nel formato *Dominio/Utente* o *Gruppodilavoro/Utente*. È necessario specificare le password corrispondenti.

Quando si specificano i dettagli di configurazione del Mirror, l'utente può anche specificare le versioni della lingua per le quali desidera scaricare le copie di aggiornamento. L'impostazione della versione della lingua è disponibile nella sezione **File > Versioni disponibili**.

4.4.1.2.4.1 Aggiornamento dal Mirror

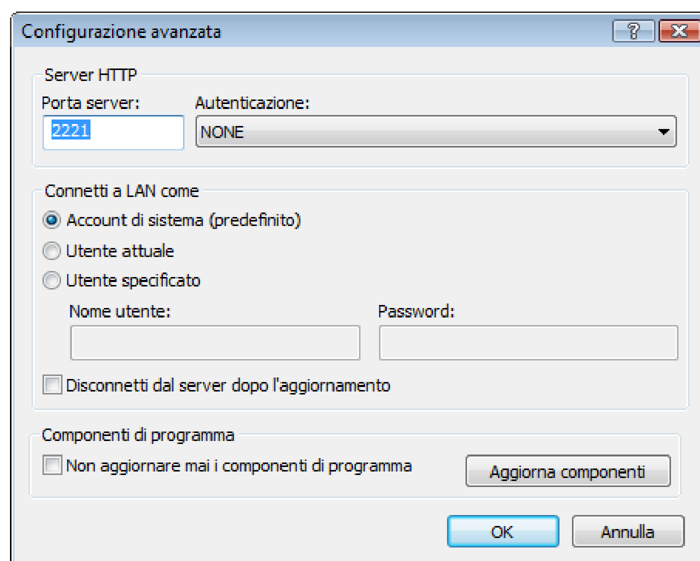
Sono disponibili due metodi di base per la configurazione del mirror: la cartella con i file di aggiornamento può essere presentata come Mirror di una cartella di rete condivisa o come Mirror di un server HTTP.

Accesso al Mirror mediante un server HTTP interno

Questa è la configurazione predefinita, specificata nella configurazione predefinita del programma. Per accedere al Mirror utilizzando il server HTTP, passare a **Configurazione aggiornamento avanzata** (la scheda **Mirror**) e scegliere l'opzione **Crea mirror di aggiornamento**.

Nella sezione **Configurazione avanzata** della scheda **Mirror** è possibile specificare la **Porta server** di ascolto del server HTTP, oltre al tipo di **Autenticazione** utilizzata dal server HTTP. Nell'impostazione predefinita, la porta del server è la **2221**. Con l'opzione **Autenticazione:** si definisce il metodo di autenticazione utilizzato per l'accesso ai file di aggiornamento. Sono disponibili le seguenti opzioni: **NESSUNO, Base** e **NTLM**. Selezionare **Base** per utilizzare la codifica base64 con l'autenticazione di base di nome utente e password. L'opzione **NTLM** consente l'uso di un metodo di codifica sicuro. Per l'autenticazione, viene utilizzato l'utente creato sulla workstation di condivisione dei file di aggiornamento. L'impostazione predefinita è **NESSUNO**, che consente l'accesso ai file di aggiornamento senza alcuna autenticazione.

Avvertenza:
Se si desidera consentire l'accesso ai file di aggiornamento tramite il server HTTP, la cartella Mirror deve essere posizionata sullo stesso computer dell'istanza di ESET Smart Security che la crea.



Al termine della configurazione del Mirror, passare alle workstation e aggiungere un nuovo server di aggiornamento nel formato **http://indirizzo_IP_del_server:2221**. A tal fine, eseguire le operazioni seguenti:

- Aprire **Configurazione avanzata di ESET Smart Security** e fare clic su **Aggiorna**.
- Fare clic su **Modifica** alla destra del menu a discesa **Server di aggiornamento** e aggiungere un nuovo server utilizzando il seguente formato: http://indirizzo_IP_del_server:2221
- Selezionare il server appena aggiunto dall'elenco dei server di aggiornamento.

Accesso al Mirror tramite le condivisioni del sistema

È innanzitutto necessario creare una cartella condivisa su un dispositivo locale o di rete. Durante la creazione della cartella per il Mirror, è necessario garantire l'accesso in scrittura all'utente che salverà i file di aggiornamento nella cartella e l'accesso in lettura a tutti gli utenti che aggiorneranno ESET Smart Security dalla cartella Mirror.

Configurare quindi l'accesso al Mirror nella sezione **Configurazione aggiornamento avanzata** (scheda **Mirror**) disattivando l'opzione **Fornisci i file di aggiornamento tramite il server HTTP interno**. Questa opzione è attivata in modo predefinito nel pacchetto di installazione del programma.

Se la cartella condivisa è su un altro computer della rete, sarà necessario specificare i dati di autenticazione per l'accesso all'altro computer. Per specificare i dati di autenticazione, passare alla Configurazione avanzata di ESET Smart Security e fare clic sulla sezione **Aggiorna**. Fare clic sul pulsante **Configurazione** quindi sulla scheda **LAN**. Questa impostazione è la stessa anche per l'aggiornamento, come illustrato nel capitolo "Connessione alla LAN".

Una volta completata la configurazione del Mirror, passare alle workstation e impostare \\UNC\PATH come server di aggiornamento. Questa operazione può essere effettuata come riportato di seguito:

- Aprire la Configurazione avanzata di ESET Smart Security e fare clic su **Aggiorna**
- Fare clic su **Modifica** accanto al Server di aggiornamento e aggiungere un nuovo server utilizzando il seguente formato \\UNC\PATH.
- Selezionare il server appena aggiunto dall'elenco dei server di aggiornamento.

NOTA:
per un funzionamento corretto, il percorso alla cartella Mirror deve essere specificato come percorso UNC. Gli aggiornamenti dalle unità mappate potrebbero non funzionare.

4.4.1.2.4.2 Risoluzione dei problemi di aggiornamento Mirror

A seconda del metodo di accesso alla cartella Mirror, è possibile che si verifichino diversi tipi di problemi. Nella maggior parte dei casi, i problemi durante un aggiornamento da un server Mirror sono causati da uno o più dei motivi seguenti: specifica non corretta delle opzioni della cartella Mirror, autenticazione non corretta dei dati nella cartella Mirror, configurazione non corretta sulle workstation locali che tentano di scaricare i file di aggiornamento dal Mirror o una combinazione di questi motivi. Di seguito è riportata una panoramica sui più frequenti problemi che possono verificarsi durante un aggiornamento dal Mirror:

- **ESET Smart Security riporta un errore di collegamento al server Mirror:** errore probabilmente causato da una specifica non corretta del server di aggiornamento (percorso di rete alla cartella Mirror) da cui le workstation locali scaricano gli aggiornamenti. Per verificare la cartella, fare clic sul menu **Start** di Windows, scegliere **Esegui**, digitare il nome della cartella e fare clic su **OK**. Dovrebbe essere visualizzato il contenuto della cartella.
- **ESET Smart Security richiede un nome utente e una password:** problema probabilmente causato dall'immissione non corretta dei dati di autenticazione (Nome utente e Password) nella sezione di aggiornamento. Nome utente e Password sono utilizzati per concedere l'accesso al server di aggiornamento dal quale il programma si aggiornerà. Verificare che i dati di autenticazione siano corretti e immessi nel formato appropriato. Ad esempio, *Dominio/Nome utente* o *Gruppo di lavoro/Nome utente*, più le password corrispondenti. Se il server Mirror è accessibile a "Tutti", non significa che sia garantito l'accesso a qualsiasi utente. Con "Tutti" non si intendono utenti non autorizzati, si intende solo che la cartella è accessibile a tutti gli utenti del dominio. Di conseguenza, se una cartella è accessibile a "Tutti", sarà comunque necessario specificare un nome utente di dominio e una password nella sezione di configurazione dell'aggiornamento.
- **ESET Smart Security riporta un errore di connessione al server Mirror:** la comunicazione sulla porta definita per l'accesso alla versione HTTP del Mirror è bloccata.

4.4.2 Come creare le attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente, selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra delle informazioni visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale**.**

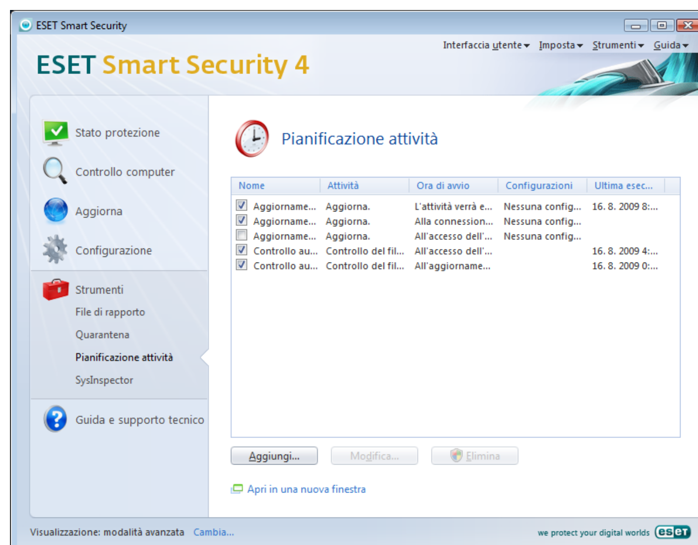
Gli aggiornamenti possono inoltre essere eseguiti come attività pianificate. Per configurare un'attività pianificata, fare clic su **Strumenti > Pianificazione attività**. Inizialmente, in ESET Smart Security sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna di queste attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, vedere "Pianificazione attività".

4.5 Pianificazione attività

Lo strumento di pianificazione attività è disponibile se in ESET Smart Security è attivata la Modalità avanzata. **Pianificazione attività** è nel menu principale di ESET Smart Security, sotto **Strumenti**. Nella pianificazione attività è disponibile un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, come data, ora e profilo di controllo predefiniti utilizzati.



Nell'impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controllo automatico file di avvio dopo l'accesso dell'utente**
- **Controllo automatico file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività **Modifica** o selezionare l'attività che si desidera modificare e fare clic sul pulsante **Modifica**.

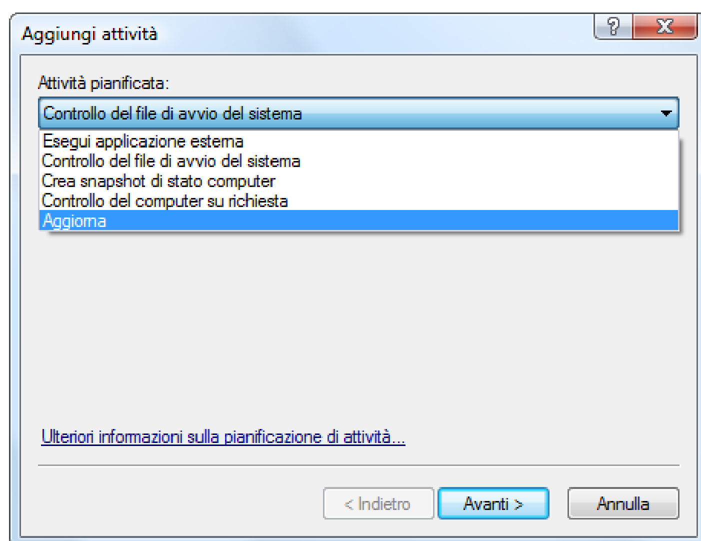
4.5.1 Scopo della pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con la configurazione e le proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

4.5.2 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi** oppure fare clic con il pulsante destro del mouse e scegliere **Aggiungi** dal menu di scelta rapida. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione esterna**
- **Manutenzione rapporto**
- **Controllo del file di avvio del sistema**
- **Controllo computer su richiesta**
- **Aggiorna**



Poiché **Scansione del computer su richiesta** e **Aggiorna** sono le attività pianificate utilizzate più spesso, di seguito verrà illustrato come aggiungere una nuova attività di aggiornamento.

Dal menu a discesa **Attività pianificata**, scegliere **Aggiorna**. Fare clic su **Avanti** e immettere il nome dell'attività nel campo **Nome attività** Selezionare la frequenza dell'attività. Sono disponibili le seguenti opzioni: **Una volta, Ripetutamente, Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi la successiva ora pianificata**
- **Esegui attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (è possibile definire l'intervallo immediatamente utilizzando la casella di scorrimento **Intervallo attività**).

Nel passaggio successivo viene visualizzata una finestra con un riepilogo completo delle attività pianificate; l'opzione **Esegui attività con i parametri specificati** dovrebbe essere automaticamente abilitata. Fare clic sul pulsante **Fine**.

Viene visualizzata una finestra di dialogo in cui è possibile scegliere i profili da utilizzare per l'attività pianificata. Qui si può specificare un profilo principale e uno alternativo, da utilizzare nel caso in cui l'attività non possa essere completata con il profilo principale. Confermare con un clic su **OK** nella finestra **Aggiorna profili**. La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

4.6 Quarantena

Lo scopo principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET Smart Security.

L'utente può scegliere di mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati ai laboratori ESET dedicati allo studio dei virus per l'analisi.



I file salvati nella cartella di quarantena possono essere visualizzati in una tabella che contiene la data e l'ora della quarantena, il percorso originale del file infetto, le dimensioni in byte, il motivo (**aggiunto dall'utente**) e il numero di minacce (ad esempio, se si tratta di un archivio che contiene più infiltrazioni).

4.6.1 Mettere i file in quarantena

Il programma mette automaticamente in quarantena i file eliminati (se l'utente non ha annullato questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti con un clic sul pulsante **Quarantena**. In tal caso il file originale non viene rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale. Fare clic con il pulsante destro del mouse nella finestra della quarantena e selezionare l'opzione **Aggiungi**.

4.6.2 Ripristino dalla quarantena

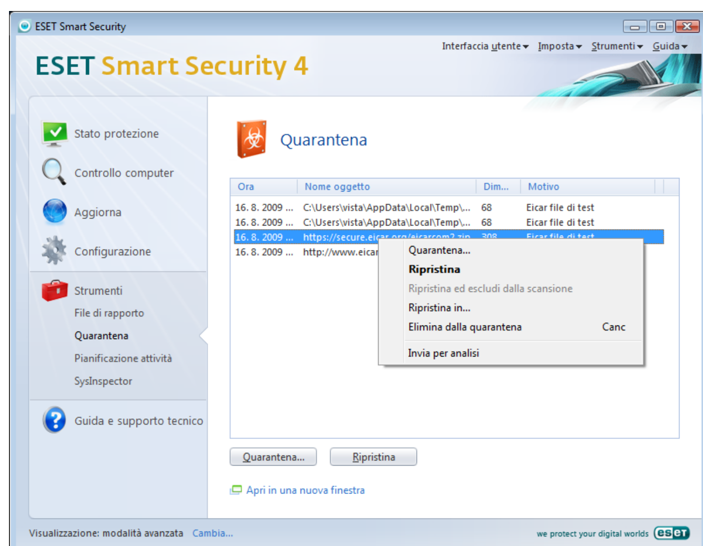
È possibile ripristinare nella posizione di origine i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina** disponibile nel menu di scelta rapida visualizzato quando si fa clic-con il pulsante destro del mouse sul file desiderato nella finestra di quarantena. Il menu di scelta rapida contiene anche l'opzione **Ripristina in**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA:
Se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

4.6.3 Invio di file dalla cartella Quarantena

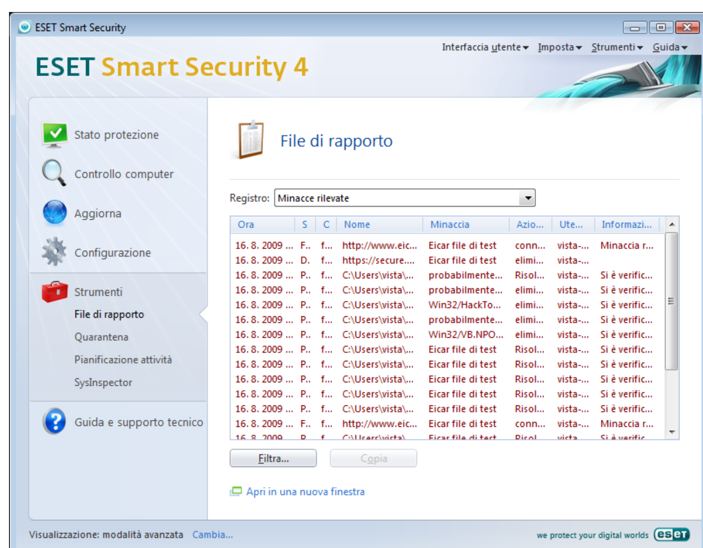
Se è stato messo in quarantena un file sospetto che non è stato rilevato dal programma, o se un file è stato valutato erroneamente come infetto (ad esempio da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file al laboratorio ESET dedicato allo studio dei virus. Per inviare un file dalla cartella di quarantena, fare clic

sul file con il pulsante destro del mouse -e selezionare **Invia per analisi** dal menu di scelta rapida.



4.7 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta uno strumento essenziale per l'analisi del sistema, per il rilevamento delle minacce e per la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i registri direttamente dall'ambiente di ESET Smart Security, nonché dai registri di archivio.



È possibile accedere ai file di rapporto dalla finestra principale di ESET Smart Security, facendo clic su **Strumenti > File di rapporto**. Selezionare il tipo di rapporto desiderato dal menu a discesa **Registro:** nella parte alta della finestra. Sono disponibili i registri seguenti:

1. **Minacce rilevate:** scegliere questa opzione per visualizzare tutte le informazioni sugli eventi relativi al rilevamento delle infiltrazioni.

2. **Eventi:** questa opzione è utile agli amministratori del sistema e agli utenti per risolvere i problemi. Tutte le azioni importanti eseguite da ESET Smart Security vengono registrate nel registro Eventi.

3. **Scansione computer su richiesta:** in questa finestra sono visualizzati i risultati di tutte le scansioni completate. Fare doppio clic-su una voce per visualizzare i dettagli del rispettivo controllo su richiesta.

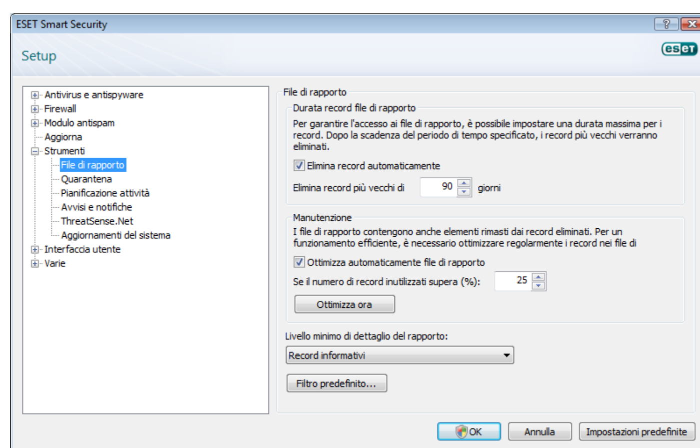
4. **Rapporto del Firewall ESET:** contiene i record di tutti i dati rilevati dal Personal firewall e a esso correlati. L'analisi del registro del firewall consente di rilevare in anticipo i tentativi di penetrazione, per evitare gli accessi non autorizzati al sistema.

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti, selezionando la voce desiderata e facendo clic sul pulsante **Copia**. Per selezionare più voci, utilizzare la combinazione di tasti CRTL e MAIUSC.

4.7.1 Manutenzione rapporto

La configurazione della registrazione di ESET Smart Security è accessibile dalla finestra principale del programma. Fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa > Strumenti > File di rapporto**. È possibile specificare le opzioni seguenti per i file di rapporto:

- **Elimina record automaticamente:** le voci del rapporto con data precedente al numero di giorni specificato vengono automaticamente eliminate
- **Ottimizza automaticamente file di registro:** consente di abilitare la deframmentazione automatica dei file di rapporto, se viene superata la percentuale specificata di record inutilizzati
- **Livello di dettaglio di registrazione minimo:** consente di specificare il livello di dettaglio di registrazione. Opzioni disponibili:
  - **Errori critici:** consente di registrare solo gli errori critici (errori di avvio di Protezione antivirus, Personal firewall e così via)
  - **Errori:** consente di registrare messaggi di errore relativi al download di un file, oltre agli errori critici
  - **Allarmi:** consente di registrare errori critici, errori generici e messaggi di allarme
  - **Record informativi:** consente di registrare messaggi informativi compresi i messaggi relativi ad aggiornamenti riusciti, oltre tutti i record riportati sopra
  - **Record diagnostici:** consente di registrare le informazioni necessarie per la configurazione dettagliata del programma e di tutti i record riportati sopra



4.8 Interfaccia utente

Le opzioni di configurazione dell'interfaccia utente di ESET Smart Security possono essere modificate in modo da impostare l'ambiente di lavoro in base alle esigenze personali. A queste opzioni di configurazione è possibile accedere dalla sezione **Interfaccia utente** della struttura di configurazione avanzata di ESET Smart Security.

Nella sezione **Elementi dell'interfaccia utente** è possibile, se necessario, passare alla modalità avanzata. In Modalità avanzata

vengono visualizzate impostazioni più dettagliate e controlli aggiuntivi per ESET Smart Security.

L'opzione **Interfaccia grafica utente** deve essere disattivata se gli elementi grafici rallentano le prestazioni del computer o causano altri problemi. Allo stesso modo, può rivelarsi necessario disattivare l'interfaccia grafica per gli utenti con problemi di vista, perché potrebbe creare conflitto con determinate applicazioni utilizzate per leggere il testo visualizzato sullo schermo.

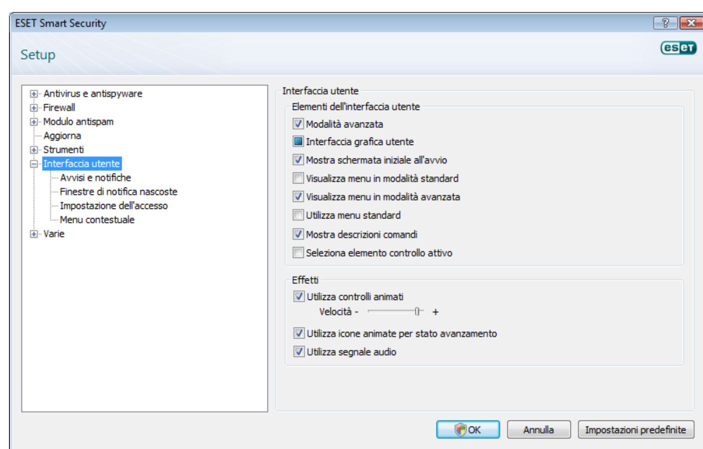
Per disattivare la schermata iniziale di ESET Smart Security, disabilitare l'opzione **Mostra schermata iniziale all'avvio**.

Nella parte superiore della finestra principale del programma ESET Smart Security, è presente un menu standard che può essere attivato o disattivato in base all'opzione **Utilizza menu standard**.

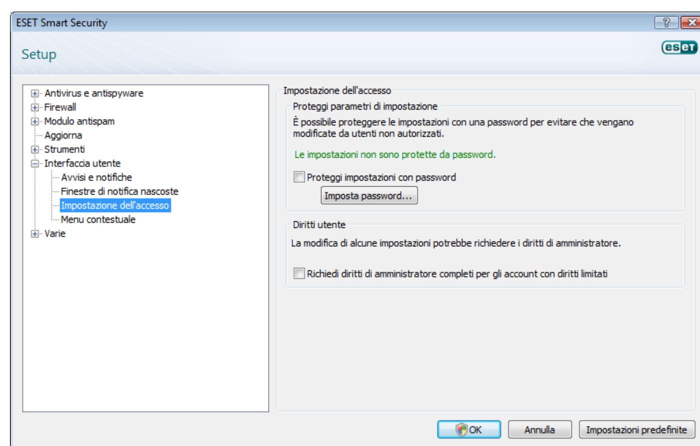
Se l'opzione **Mostra descrizioni comandi** è attivata, verrà visualizzata una breve descrizione quando si passa con il cursore sulle singole opzioni. Scegliendo l'opzione **Seleziona elemento controllo attivo**, verrà evidenziato l'elemento presente al momento nell'area attiva del cursore del mouse. L'elemento evidenziato verrà attivato con un clic del mouse.

Per ridurre o aumentare la velocità degli effetti animati, scegliere l'opzione **Utilizza controlli animati** e spostare il cursore **Velocità** a sinistra o a destra.

Per attivare l'utilizzo delle icone animate per visualizzare l'avanzamento delle diverse operazioni, selezionare la casella **Utilizza icone animate per stato avanzamento**. Per riprodurre un segnale acustico di allarme in occasione di eventi importanti, scegliere l'opzione **Utilizza segnale audio**.



Le funzioni di **Interfaccia utente** comprendono anche l'opzione per proteggere la configurazione di ESET Smart Security con una password. Questa opzione è nel sottomenu **Configurazione protezione** sotto **Interfaccia utente**. Per garantire la massima sicurezza del sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per impostare una password a protezione dei parametri di configurazione, fare clic su **Immetti password**.



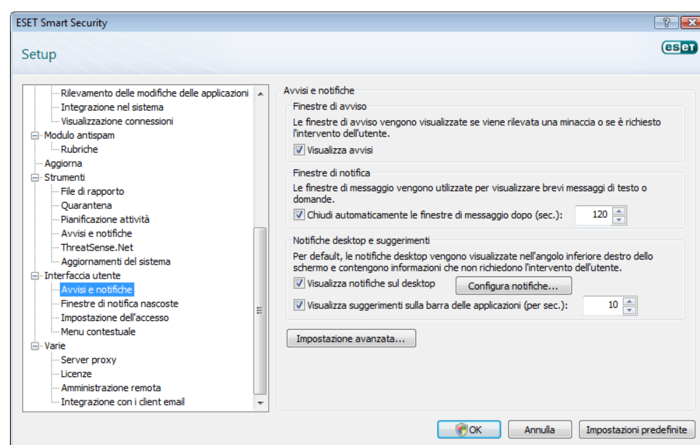
4.8.1 Avvisi e notifiche

La sezione **Impostazione di avvisi e notifiche** in **Interfaccia utente**, consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema in ESET Smart Security.

La prima voce da considerare è **Visualizza avvisi**. Se questa opzione viene disabilitata, tutte le finestre di avviso vengono annullate, per cui è adatta solo a un numero limitato di situazioni specifiche. Per la maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).

Per chiudere automaticamente le finestre pop-up dopo un determinato periodo di tempo, selezionare l'opzione **Chiudi automaticamente le finestre di messaggio dopo (sec.)**. Se non vengono chiuse manualmente dall'utente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Le notifiche visualizzate sul desktop e i suggerimenti sono strumenti esclusivamente informativi, che non consentono né richiedono l'interazione dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo inferiore destro della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare l'opzione **Visualizza notifiche sul desktop**. Per modificare opzioni più dettagliate, come l'orario di visualizzazione notifica e la trasparenza della finestra, fare clic sul pulsante **Configura notifiche...** Per visualizzare in anteprima il funzionamento delle notifiche, fare clic sul pulsante **Anteprima**. Per configurare la durata della visualizzazione dei suggerimenti, vedere l'opzione **Visualizza suggerimenti sulla barra delle applicazioni (per sec.)**.



Fare clic su **Configurazione avanzata** per inserire opzioni di configurazione aggiuntive in **Avvisi e notifiche**, tra cui **Visualizza solo le notifiche che richiedono l'interazione dell'utente**. L'opzione consente di attivare/disattivare la visualizzazione di avvisi e notifiche che non richiedono l'intervento dell'utente. Per eliminare tutte le notifiche non interattive, selezionare Visualizza solo le notifiche che richiedono l'interazione dell'utente quando le applicazioni vengono eseguite in

modalità schermo intero. Dal menu a discesa Livello di dettaglio minimo per gli eventi da visualizzare è possibile selezionare la priorità iniziale di avvisi e notifiche da visualizzare.

L'ultima funzione di questa sezione è la possibilità di specificare gli indirizzi di notifica per un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente:** è possibile definire chi riceverà notifiche importanti da ESET Smart Security 4. In genere si tratterà di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, purché tutte le notifiche di sistema vengano inviate all'amministratore.

4.9 ThreatSense.Net

Il sistema di allarme immediato ThreatSense.Net è uno strumento che informa in modo tempestivo e continuato ESET sulle nuove infiltrazioni. Il sistema di allarme immediato bidirezionale ThreatSense.Net ha un unico scopo: migliorare la protezione offerta da ESET. Il metodo migliore per garantire che le nuove minacce vengano riconosciute da ESET non appena appaiono è rappresentato dal "collegamento" con il maggior numero possibile di clienti, da utilizzare come "esploratori di minacce". Sono disponibili due opzioni:

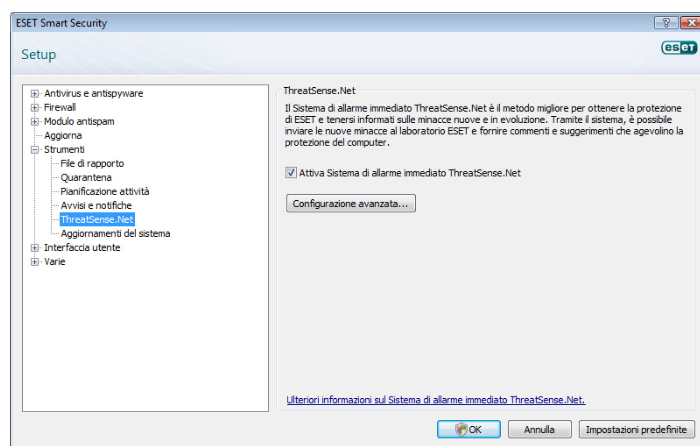
- È possibile decidere di non abilitare il sistema di allarme immediato ThreatSense.Net. Non si perderà alcuna funzionalità del software e si otterrà comunque la migliore protezione che ESET è in grado di offrire.

- È possibile configurare il sistema di allarme immediato per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente del nuovo codice dannoso, in un unico file. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto ad ESET per aggiornare le proprie capacità di rilevamento delle minacce. Il sistema di allarme immediato ThreatSense.Net raccoglie le informazioni sul computer degli utenti relative alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso del il file, il nome del file, informazioni su data e ora, il processo in corrispondenza del quale è apparsa la minaccia sul computer e informazioni sul sistema operativo del computer. Alcune delle informazioni possono includere dati personali sull'utente del computer, come il nome utente in un percorso di directory e così via. Un esempio delle informazioni sul file inviate è riportato di seguito.

Sebbene esista la possibilità che occasionalmente vengano trasmesse informazioni sull'utente o sul computer ai laboratori antivirus di ESET, tali informazioni non saranno utilizzate per ALCUNO scopo diverso da quello di consentire ad ESET di rispondere in modo immediato alle nuove minacce.

Nell'impostazione predefinita, ESET Smart Security è configurato in modo da proporre una richiesta di conferma prima di inviare i file sospetti per l'analisi dettagliata ai laboratori ESET. È importante notare che i file con determinate estensioni, come .doc o .xls sono sempre esclusi dall'invio, anche qualora fosse rilevata una minaccia al loro interno. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o l'organizzazione di cui fa parte l'utente desidera evitare di inviare.

La configurazione di ThreatSense.Net è accessibile dalla struttura di configurazione avanzata, in **Strumenti > ThreatSense.Net**. Selezionare la casella di controllo **Attiva Sistema di allarme immediato ThreatSense.Net**. Ciò consentirà di attivarlo e di fare quindi clic sul pulsante **Configurazione avanzata**.

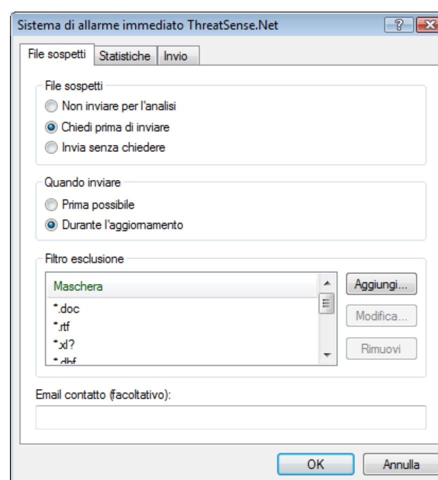


4.9.1 File sospetti

Nella scheda **File sospetti** è possibile configurare il modo in cui le minacce vengono inviate al laboratorio ESET per l'analisi.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai laboratori ESET. Se viene individuata un'applicazione dannosa, verrà aggiunta al prossimo aggiornamento delle firme antivirali.

L'invio dei file può essere impostato per essere eseguito automaticamente senza l'intervento dell'utente. Se viene selezionata questa opzione, i file sospetti vengono inviati in background. Per conoscere i file inviati per l'analisi e confermare l'invio, selezionare l'opzione **Chiedi prima di inviare**.



Se non si desidera inviare i file, selezionare **Non inviare per l'analisi**. Se si sceglie di non inviare file per l'analisi, questa decisione non influisce sull'invio delle informazioni statistiche a ESET. Le informazioni statistiche sono configurate in una sezione di impostazione a parte, descritta nel capitolo successivo.

Quando inviare
I file sospetti vengono inviati ai laboratori ESET per l'analisi appena possibile. Ciò è consigliabile se si dispone di una connessione permanente a Internet e se i file sospetti possono essere inviati in tempi brevi. L'altra opzione consiste nell'inviare i file sospetti **Durante l'aggiornamento**. Se viene selezionata questa seconda opzione, i file sospetti vengono raccolti e caricati sui server del sistema di allarme immediato durante un aggiornamento.

Filtro esclusione
Non è necessario che vengano inviati per l'analisi tutti i file. L'opzione Filtro esclusione consente di escludere dall'invio determinati file e/o cartelle. È utile, ad esempio, escludere file che possono contenere informazioni potenzialmente riservate, ovvero documenti o fogli di calcolo. I tipi di file più comuni sono esclusi per impostazione predefinita (Microsoft Office, OpenOffice). Se necessario, è possibile incrementare l'elenco dei file esclusi.

Email contatto
L'indirizzo email di contatto viene inviato a ESET insieme ai file sospetti e può essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni sui file ai fini dell'analisi. Dopo l'invio, l'utente non riceve una risposta da ESET, a meno che non siano richieste ulteriori informazioni.

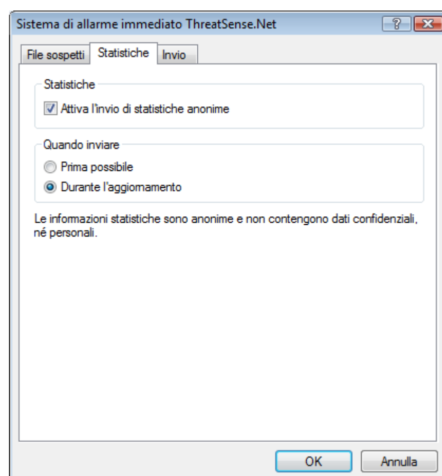
4.9.2 Statistiche

Il sistema di allarme immediato ThreatSense.Net raccoglie informazioni anonime sul computer in relazione alle nuove minacce rilevate. Le informazioni possono comprendere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione di ESET Smart Security, la versione del sistema operativo in uso e il percorso del file. Le statistiche vengono inviate in genere ai server ESET una o due volte al giorno.

Di seguito è riportato un esempio di pacchetto di statistiche inviato:

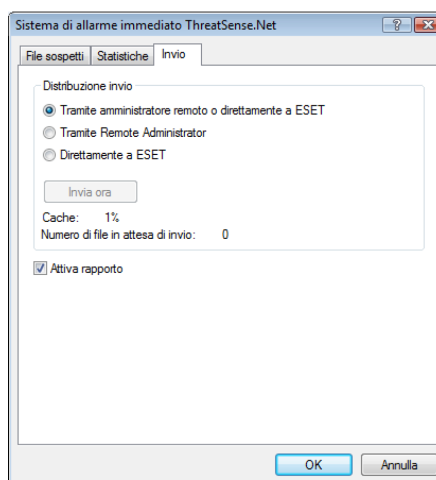
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

Quando inviare
Nella sezione **Quando inviare** è possibile definire quando inviare le informazioni statistiche. Se si sceglie di eseguire l'invio **Prima possibile**, le informazioni statistiche verranno inviate subito dopo essere state create. Questa impostazione è adatta nel caso in cui si utilizzi una connessione permanente a Internet. Se si seleziona l'opzione **Durante l'aggiornamento**, le informazioni statistiche vengono salvate per essere quindi inviate tutte insieme al successivo aggiornamento.



4.9.3 Invio

In questa sezione, è possibile scegliere se inviare file e informazioni statistiche tramite il Remote Administrator ESET o direttamente a ESET. Per essere certi che le informazioni statistiche e i file sospetti vengano recapitati a ESET, selezionare l'opzione **Tramite Remote Administrator o direttamente a ESET**. In tal modo i file e le statistiche vengono inviati con tutti gli strumenti disponibili. Impostando l'invio di file sospetti tramite il Remote Administrator, i file e le statistiche vengono inviati al server di amministrazione remota, che assicura il successivo invio ai laboratori ESET per lo studio dei virus. Se viene selezionata l'opzione **Direttamente a ESET**, tutti i file sospetti e le informazioni statistiche vengono inviati al laboratorio ESET per lo studio dei virus direttamente dal programma.



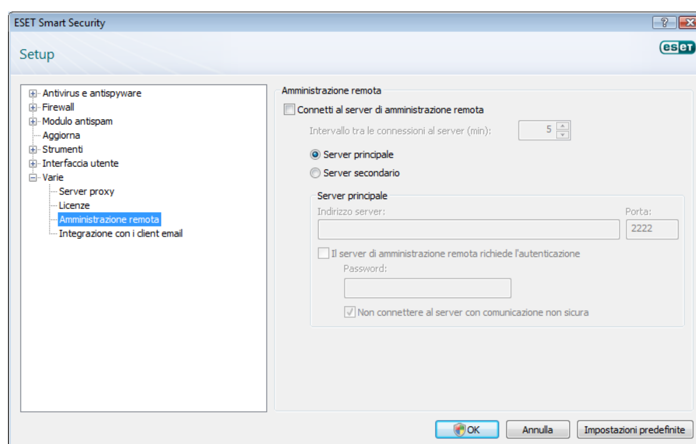
Se esistono file in attesa di invio, è possibile attivare il pulsante **Invia ora** in questa finestra di configurazione. Fare clic sul pulsante per inviare immediatamente i file e i dati statistici.

Selezionare l'opzione **Attiva registrazione** per attivare la registrazione dell'invio di dati statistici e file. Dopo ogni invio di file sospetto o di un'informazione statistica, viene creata una voce nel registro eventi.

4.10 Amministrazione remota

L'amministrazione remota è uno strumento potente per la gestione dei criteri di sicurezza e per avere una panoramica sulla gestione globale della sicurezza all'interno della rete. È particolarmente utile quando si applica a reti di una certa dimensione. L'amministrazione remota non solo garantisce un aumento del livello di sicurezza, ma è anche uno strumento facile da utilizzare per l'amministrazione di ESET Smart Security sulle workstation client.

Le opzioni di configurazione dell'amministrazione remota sono disponibili nella schermata principale di ESET Smart Security. Fare clic su **Configurazione > Immettere struttura di impostazione avanzata completa > Varie > Amministrazione remota**.



Nella finestra Configurazione è possibile attivare la modalità di amministrazione remota, selezionando la casella di controllo **Connetti al server di amministrazione remota**. È possibile quindi accedere alle altre opzioni descritte di seguito:

- **Indirizzo server:** l'indirizzo di rete del server su cui è installato il server di amministrazione remota.
- **Porta:** questo campo contiene la porta predefinita utilizzata per la connessione al server. È consigliabile conservare l'impostazione predefinita della porta su 2222.
- **Intervallo tra le connessioni al server (min):** indica la frequenza con cui ESET Smart Security si connette al server ERA per inviare

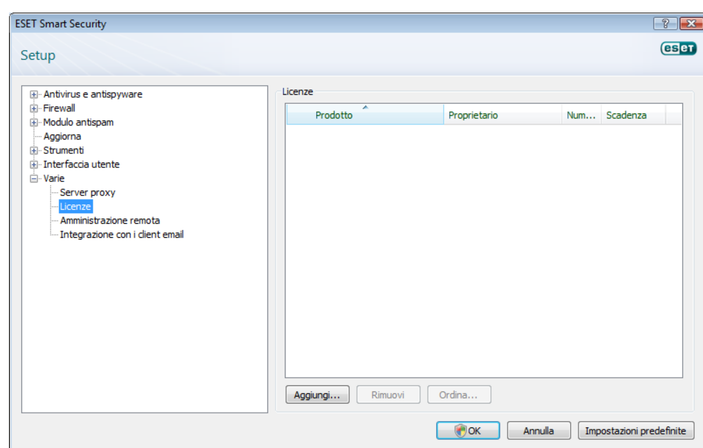
i dati. In altri termini, le informazioni vengono inviate in base agli intervalli di tempo definiti in questo campo. Se il valore impostato è 0, le informazioni vengono inviate ogni 5 secondi.

- **Il server di amministrazione remota richiede l'autenticazione:** consente di immettere una password per la connessione al server di amministrazione remota, se necessario.

Scegliere **OK** per confermare le modifiche e applicare le impostazioni. ESET Smart Security utilizza queste impostazioni per connettersi al server remoto.

4.11 Licenza

Nella sezione **Licenze** è possibile gestire le chiavi di licenza per ESET Smart Security e per altri prodotti ESET come il Remote Administrator ESET, ESET NOD32 per Microsoft Exchange e così via. Dopo l'acquisto, le chiavi di licenza vengono fornite insieme a Nome utente e Password. Per **aggiungere o rimuovere** una chiave di licenza, fare clic sul pulsante corrispondente della finestra di gestione delle licenze. È possibile accedere alla gestione licenze dalla struttura di configurazione avanzata in **Varie > Licenze**.



La chiave di licenza è un file di testo contenente informazioni sul prodotto acquistato: il proprietario, il numero di licenze e la data di scadenza.

Nella finestra di gestione delle licenze è possibile caricare e visualizzare il contenuto di una chiave di licenza utilizzando il pulsante **Aggiungi**. Le informazioni contenute vengono visualizzate nella finestra. Per eliminare i file di licenza dall'elenco, fare clic su **Rimuovi**.

Se una chiave di licenza è scaduta e si desidera acquistarne un rinnovo, fare clic sul pulsante **Ordina**. L'utente verrà reindirizzato al negozio in linea.

5. Utente avanzato

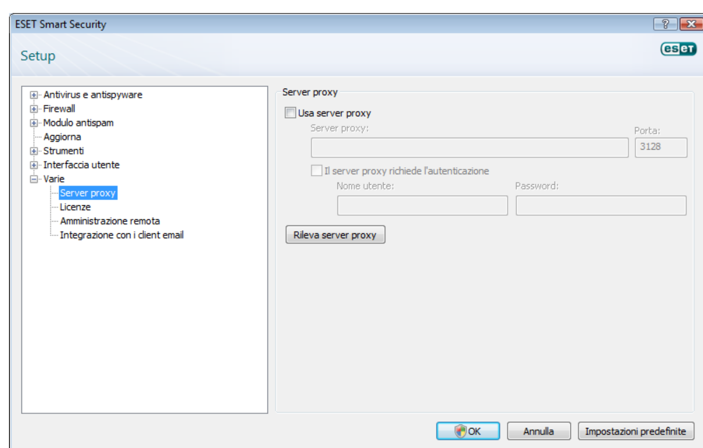
In questo capitolo vengono descritte le funzioni di ESET Smart Security progettate per gli utenti più esperti. Alle opzioni di configurazione di queste funzioni è possibile accedere solo in modalità avanzata. Per passare alla modalità avanzata, fare clic su **Attiva/disattiva modalità avanzata** nell'angolo inferiore sinistro della finestra del programma principale oppure premere CTRL + M sulla tastiera.

5.1 Impostazione del server proxy

In ESET Smart Security la configurazione del server proxy è disponibile in due diverse sezioni all'interno della struttura Configurazione avanzata.

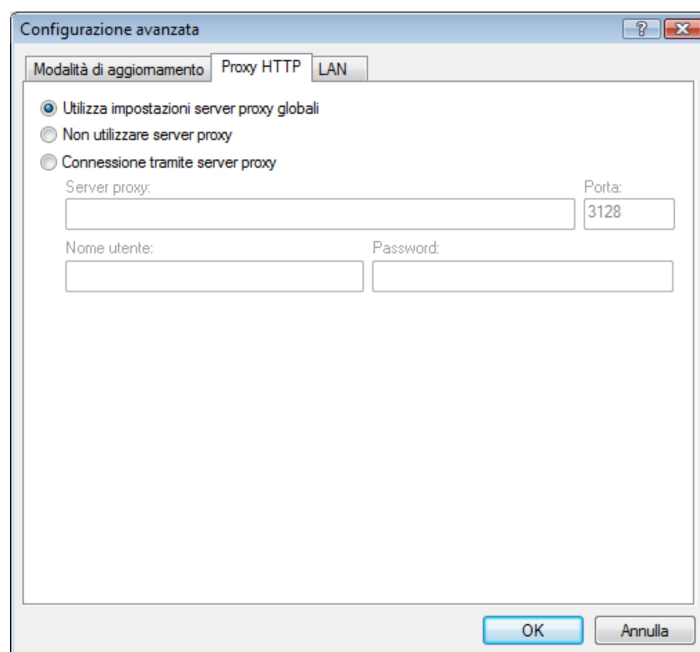
Le impostazioni del server proxy si possono configurare sotto **Varie > Server proxy**. Se si specifica il server proxy a questo livello, si definiscono globalmente le impostazioni del server proxy per l'intera applicazione ESET Smart Security. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy a questo livello, selezionare la casella di controllo **Usa server proxy**, quindi immettere l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.



Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi. Fare clic sul pulsante **Rileva server proxy** per rilevare automaticamente e immettere le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer. Con questa funzione non si rilevano i dati di autenticazione (Nome utente e Password), che devono essere immessi dall'utente.

È possibile specificare le impostazioni del server proxy anche all'interno di **Configurazione aggiornamento avanzata** (sezione **Aggiorna** della struttura Configurazione avanzata). L'impostazione viene applicata al profilo di aggiornamento specificato ed è consigliata per i computer portatili, che spesso ricevono aggiornamenti delle firme antivirali da altre posizioni sulla rete. Per ulteriori informazioni su questa impostazione, vedere la Sezione 4.4, "Aggiornamento del programma".



5.2 Esportazione o importazione di impostazioni

È possibile eseguire l'esportazione e l'importazione della configurazione corrente di ESET Smart Security in modalità avanzata sotto **Configurazione**.

Sia per l'importazione che per l'esportazione si utilizzano file .xml. Queste operazioni sono utili per eseguire una copia di backup della configurazione corrente di ESET Smart Security da utilizzare in un secondo momento (per qualsiasi motivo). La funzione di esportazione delle impostazioni sarà apprezzata in particolare da chi desidera utilizzare la propria configurazione preferita di ESET Smart Security su più sistemi (in cui importare il file .xml).



5.2.1 Esportazione delle impostazioni

L'esportazione della configurazione è molto semplice. Per salvare la configurazione corrente di ESET Smart Security, fare clic su **Configurazione > Importa ed esporta impostazioni**. Selezionare l'opzione **Esporta impostazioni** e immettere il nome del file di configurazione. Scegliere il percorso sul computer in cui salvare il file di configurazione.

5.2.2 Importazione delle impostazioni

Le operazioni per l'importazione di una configurazione sono molto simili. Anche in questo caso, selezionare **Importa ed esporta impostazioni**, quindi selezionare l'opzione **Importa impostazioni**. Fare clic sul pulsante **...** e cercare il file di configurazione da importare.

5.3 Riga di comando

Il modulo antivirus di ESET Smart Security può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat").

È possibile utilizzare i parametri e le opzioni riportate di seguito quando viene eseguito un controllo su richiesta dalla riga di comando:

Opzioni generali:

– help	mostra Guida ed esci
– version	mostra informazioni sulla versione ed esci
– base-dir = CARTELLA	carica moduli da CARTELLA
– quar-dir = CARTELLA	Cartella QUARANTENA
– aind	mostra indicatore di attività

Destinazioni:

– files	esegui scansione dei file (impostazione predefinita)
– no-files	non eseguire scansione dei file
– boots	esegui scansione dei settori di avvio (impostazione predefinita)
– no-boots	non eseguire scansione dei settori di avvio
– arch	esegui scansione degli archivi (impostazione predefinita)
– no-arch	non eseguire scansione degli archivi
– max-archive-level = LIVELLO	LIVELLO di nidificazione massima degli archivi
– scan-timeout = LIMITE	esegui controllo degli archivi al massimo per LIMITE secondi. Se la durata della scansione raggiunge questo limite, la scansione dell'archivio viene interrotta e si passa al file successivo
– max-arch-size = DIMENSIONE	esegui controllo solamente della DIMENSIONE dei primi byte predefinita 0 = illimitato
– mail	esegui scansione dei file di e-mail
– no-mail	non eseguire scansione dei file di e-mail
– sfx	esegui controllo degli archivi-autoestraenti
– no-sfx	non eseguire controllo degli archivi-autoestraenti
– rtp	eseguire scansione degli eseguibili compressi
– no-rtp	non eseguire scansione degli eseguibili compressi
– exclude = CARTELLA	escludi CARTELLA dal controllo
– subdir	esegui scansione delle sottocartelle (impostazione predefinita)
– no-subdir	non eseguire scansione delle sottocartelle
– max-subdir-level = LIVELLO	LIVELLO di nidificazione massima delle sottocartelle (valore predefinito 0 = illimitato)
– symlink	segui collegamenti simbolici (impostazione predefinita)
– no-symlink	ignora collegamenti simbolici
– ext-remove = ESTENSIONI	
– ext-exclude = ESTENSIONI	escludi dalla scansione le ESTENSIONI delimitate da due punti

Metodi:

– adware	esegui scansione di Adware/Spyware/Riskware
– no-adware	non eseguire scansione di Adware/Spyware/Riskware
– unsafe	esegui scansione delle applicazioni potenzialmente pericolose
– no-unsafe	non eseguire scansione delle applicazioni potenzialmente pericolose
– unwanted	esegui scansione delle applicazioni potenzialmente indesiderate
– no-unwanted	non eseguire scansione delle applicazioni potenzialmente indesiderate
– pattern	utilizza le firme
– no-pattern	non utilizzare le firme
– heur	attiva l'euristica
– no-heur	disattiva l'euristica
– adv-heur	attiva Euristica avanzata
– no-adv-heur	disattiva Euristica avanzata

Pulizia:

– action = AZIONE Azioni disponibili: none, clean, prompt (nessuna, disinfetta, chiedi)	esegui AZIONE sugli oggetti infetti
– quarantine (integra AZIONE)	copia i file infettati in Quarantena
– no-quarantine	non copiare file infettati in Quarantena

Registro:

– log-file = FILE	registra output in un FILE
– log-rewrite	sovrascrivi file di output (predef.: aggiungi al file)
– log-all	registra anche file puliti
– no-log-all	non registrare file puliti (impostazione predefinita)

I codici restituiti dalla scansione possono essere i seguenti:

0 – nessuna minaccia rilevata
1 – minaccia rilevata ma non pulita
10 – sono rimasti alcuni file infetti
101 – errore archivio
102 – errore accesso
103 – errore interno

NOTA:
I codici restituiti superiori a 100 indicano che non è stato eseguito il controllo del file, che potrebbe quindi essere infetto.

5.4 ESET SysInspector

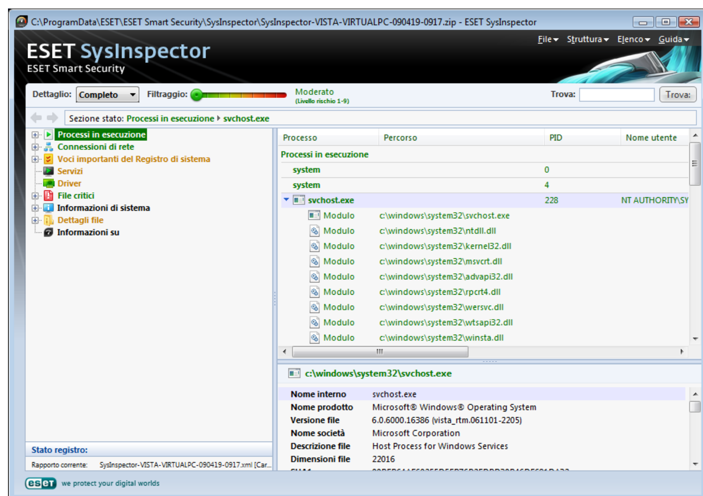
L'applicazione ESET SysInspector controlla il computer in modo approfondito e visualizza i dati raccolti in modo globale. Il possesso di informazioni su driver e applicazioni, su connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Sono disponibili due varianti di SysInspector nella famiglia di prodotti ESET. L'applicazione portatile (SysInspector.exe) può essere scaricata gratuitamente dal sito Web ESET. La variante integrata è inclusa in ESET Smart Security 4. Per aprire la sezione SysInspector, attivare la modalità di visualizzazione avanzata nella parte in basso a sinistra, quindi fare clic su **Strumenti > SysInspector**. Le due varianti sono identiche quanto a funzionamento e presentano gli stessi controlli di programma. L'unica differenza risiede nella modalità di gestione dell'output. Nell'applicazione portatile, è possibile esportare il rapporto sul sistema in un file XML e salvare tale file su disco. Tale operazione è possibile anche nella versione integrata di SysInspector. In aggiunta, è possibile memorizzare lo stato del sistema direttamente in **ESET Smart Security 4 > Strumenti > SysInspector** (per ulteriori informazioni, vedere 5.4.1.4. SysInspector come componente di ESS).

Durante il controllo del computer da parte di ESET SysInspector è necessario attendere. Il processo può richiedere da 10 secondi fino a diversi minuti a seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer.

5.4.1 Interfaccia utente e utilizzo dell'applicazione

Per agevolarne l'utilizzo la finestra principale è stata divisa in quattro sezioni. I comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra, nella parte centrale, è disponibile la finestra Descrizione, infine, nella parte inferiore destra della schermata viene visualizzata la finestra Dettagli.



5.4.1.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector

File
Facendo clic su questa voce è possibile memorizzare lo stato attuale del rapporto per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Se si desidera pubblicare il rapporto, consigliamo di generarlo in modo che risulti idoneo all'invio. In questa forma, il rapporto omette le informazioni riservate.

Nota: *È possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale.*

Struttura
Consente di incrementare o chiudere tutti i nodi

Elenco
Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, come la ricerca online di materiale informativo.

Importante: *gli elementi evidenziati in rosso sono sconosciuti, per questo motivo il programma li segna come potenzialmente pericolosi. Se un elemento è in rosso, non significa automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.*

Aiuto
Contiene informazioni sull'applicazione e le relative funzioni.

Dettaglio
Influenza le informazioni visualizzate nelle altre sezioni della finestra principale, semplificando l'utilizzo del programma. Nella modalità di base si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità Media il programma visualizza i dettagli meno utilizzati, mentre nella modalità Completa ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi molto specifici.

Filtraggio elementi
Filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio attuale, visualizzando solo gli elementi che risultano più sospetti del livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi che si trovano nell'intervallo di rischio da 6 a 9 rappresentano un rischio per la sicurezza. Quando il programma ha rilevato un elemento di questo tipo, si consiglia di eseguire la scansione del sistema con ESET Online scanner, se non si utilizzano alcune delle soluzioni di protezione di ESET. ESET Online scanner è un servizio gratuito ed è disponibile all'indirizzo http://www.eset.eu/online-scanner.

Nota: *il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.*

Trova
L'opzione Trova può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o a una parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna
Facendo clic sulla freccia indietro o avanti è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione.

Sezione Stato
Visualizza il nodo corrente nella finestra di spostamento.

5.4.1.2 Navigare in ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, eventuali ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo o in alternativa selezionare ⊞ o ⊟ , accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, si possono trovare vari dettagli su ciascun nodo presente nella finestra Descrizione. Navigando tra gli elementi della finestra Descrizione, è possibile visualizzare maggiori dettagli per ciascun elemento nella finestra Dettagli.

Seguono le descrizioni dei nodi principali presenti nella finestra di spostamento e le informazioni relative delle finestre Descrizione e Dettagli.

Processi in esecuzione
Questo nodo contiene informazioni sulle applicazioni e i processi in esecuzione al momento di generare il rapporto. Nella finestra Descrizione, si trovano dettagli aggiuntivi per ciascun processo, come le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione, il livello di rischio del file e così via.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o l'hash relativo.

Nota: *Un sistema operativo è basato su diversi componenti kernel, in esecuzione 24 ore su 24, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli, risultano sicuri per il sistema e pertanto sono considerati corretti.*

Connessioni di rete
La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È anche possibile controllare gli indirizzi IP assegnati all'assegnazione DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o l'hash relativo.

Voci importanti del Registro di Sistema
Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, come quelle che indicano i programmi di avvio, oggetti browser helper (BHO), e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci

di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi
La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver
Un elenco di driver installati nel sistema.

File critici
Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows®.

Informazioni di sistema
Contiene informazioni dettagliate sull'hardware e software, oltre a informazioni sulle variabili d'ambiente impostate e i diritti dell'utente.

Dettagli file
Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su
Informazioni su ESET SysInspector

5.4.1.3 Confronta rapporti

La funzione Confronta consente di confrontare due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione adatta se si desidera rilevare le modifiche nel sistema: ad esempio, l'utente desidera individuare l'attività del codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Selezionare **File -> Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere successivamente aperti e visualizzati. Per aprire un rapporto esistente, utilizzare il menu **File -> Apri rapporto**. Nella finestra principale del programma ESET SysInspector visualizza sempre un rapporto alla volta.

Se si confrontano due rapporti, in realtà si confronta un rapporto attualmente attivo con uno salvato in un file. Per confrontare due rapporti, utilizzare l'opzione **File -> Confronta rapporti** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel risultante rapporto, detto comparativo, saranno visualizzate solo le differenze tra i due.

Nota: *Se si confrontano due file di rapporto, selezionando File -> Salva rapporto e salvandoli in un file ZIP, entrambi i file verranno salvati. Se si apre il file successivamente, i rapporti contenuti verranno automaticamente confrontati.*

Accanto agli elementi visualizzati, SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.
Gli elementi contrassegnati con − si trovano solo nel rapporto attivo e non erano presenti nel rapporto comparativo aperto. Tuttavia, gli elementi contrassegnati con + erano presenti solo nel rapporto aperto e mancavano in quello attivo.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

+ nuovo valore, non presente nel rapporto precedente

sezione della struttura ad albero contenente nuovi valori

− valore rimosso, presente solo nel rapporto precedente

sezione della struttura ad albero contenente valori rimossi

valore/file modificato

sezione della struttura ad albero contenente valori/file modificati

il livello di rischio è diminuito/ere maggiore nel rapporto precedente

il livello di rischio è aumentato/era minore nel rapporto precedente

La sezione di descrizione visualizzata nell'angolo inferiore sinistro descrive tutti i simboli e mostra i nomi dei rapporti confrontati.

Stato registro:

Rapporto corrente:	SysInspector-WINVISTAX64SP1-090815-1906.xml [Caricato-ZIP]
Privato:	Sì
Rapporto precedente:	SysInspector-WINVISTAX64SP1-090815-1916.xml [Caricato]
Privato:	Sì
Confronta:	[Risultato confronto]

Confronta legenda icone:

+ Elemento aggiunto	Elementi aggiunti nel ramo
− Elemento rimosso	Elementi rimossi dal ramo
File sostituito	Elementi aggiunti o rimossi dal ramo
Stato abbassato	
Stato aumentato	File sostituiti nel ramo

Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio:
generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver effettuato le modifiche al sistema, aprire SysInspector ed eseguire la generazione di un nuovo rapporto. Salvarlo in un file denominato current.xml.

Al fine di rilevare le modifiche tra i due rapporti, andare a **File -> Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza solo le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

5.4.1.4 SysInspector come componente di ESET Smart Security 4

Per aprire la sezione SysInspector in ESET Smart Security 4, fare clic su **Strumenti > SysInspector**. Il sistema di gestione della finestra di SysInspector è simile a quello dei rapporti di controllo del computer o delle attività pianificate. Tutte le operazioni con i rapporti del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di SysInspector contiene informazioni di base sui rapporti creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato il rapporto e lo stato dello stesso.

Per eseguire le operazioni **Confronta, Aggiungi**, o **Rimuovi** sugli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di SysInspector. Tali opzioni sono disponibili anche dal menu contestuale. Per visualizzare il rapporto di sistema selezionato, utilizzare l'opzione **Visualizza** del menu contestuale. Per esportare il rapporto selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...** Segue una descrizione dettagliata delle opzioni disponibili:

Confronta: consente di confrontare due rapporti esistenti. È consigliabile se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due rapporti da confrontare.

Aggiungi crea un nuovo record. Prima è necessario inserire un breve commento sul record. Per visualizzare l'avanzamento percentuale della creazione del rapporto (relativamente al rapporto in corso di generazione), fare riferimento alla colonna Stato. Tutti i rapporti completati sono contrassegnati dallo stato Data di creazione.

Rimuovi: rimuove le porte dall'elenco

Mostra: visualizza il rapporto selezionato. In alternativa, è possibile

fare doppio clic sulla voce selezionata.

Esporta...: salva la voce selezionata in un file XML (anche in una versione compressa)

5.5 ESET SysRescue

ESET Recovery CD (ERCD) è un'utilità che consente di creare un disco di avvio contenente ESET Smart Security 4 (ESS). Il vantaggio principale di ESET Recovery CD è dato dal fatto che ESS viene eseguito indipendentemente dal sistema operativo che lo ospita e al tempo stesso dispone dell'accesso diretto al disco e all'intero file system. Per questo motivo, è possibile rimuovere infiltrazioni che in una situazione ordinaria non avrebbero potuto essere eliminate, ad esempio, durante l'esecuzione del sistema operativo.

5.5.1 Requisiti minimi

ESET SysRescue (ESR) è eseguibile su Microsoft Windows Preinstallation Environment (Windows PE) versione 2.x, basato su Windows Vista. Windows PE è incluso nel pacchetto gratuito Windows Automated Installation Kit (Windows AIK) e pertanto deve essere installato prima di procedere alla creazione di ESR. A causa del supporto della versione a 32 bit di Windows PE, è possibile creare ESR solo nella versione di ESS/ENA a 32 bit. ESR supporta Windows AIK 1.1 e versioni successive. ESR è disponibile per ESS/ENA 4.0 e versioni successive.

5.5.2 Come creare un CD di ripristino

Se si dispone dei requisiti minimi per la creazione di ESET SysRescue (ESR) CD, l'operazione verrà completata senza difficoltà. Per avviare la procedura guidata di ESR, fare clic su **Start > Programmi > ESET > ESET Smart Security 4 > ESET SysRescue**.

Innanzitutto, la procedura guidata rileva la presenza di Windows AIK e di un dispositivo adatto alla creazione di un supporto di avvio.

Al passaggio successivo, selezionare il supporto di destinazione in cui si desidera posizionare ESR. Oltre a CD/DVD/USB è possibile scegliere di salvare ESR in un file ISO. Successivamente, sarà possibile masterizzare l'immagine ISO su CD/DVD oppure utilizzarla in altro modo (ad esempio, in ambienti virtuali, quali VmWare o Virtualbox).

Dopo aver specificato tutti i parametri, nell'ultimo passaggio della procedura guidata di ESET SysRescue viene visualizzata un'anteprima della compilazione. Verificare i parametri e avviare la compilazione. Le opzioni disponibili includono:

Cartelle
ESET Antivirus
Avanzate
Supporto USB di avvio
Masterizzazione

5.5.2.1 Cartelle

Cartella temporanea è una cartella di lavoro per i file richiesti dalla compilazione di ESET SysRescue.

Cartella ISO è una cartella in cui vengono salvati, al termine della compilazione, i file ISO.

L'elenco presente in questa scheda riporta tutte le unità di rete locali e mappate insieme allo spazio disponibile rimanente. Se alcune cartelle si trovano in un'unità che non dispone di spazio sufficiente, si consiglia di selezionare un'unità alternativa che disponga di maggiore spazio. In caso contrario, è possibile che la compilazione si interrompa in modo anomalo a causa della mancanza di spazio libero su disco.

Applicazioni esterne
Consente di specificare programmi aggiuntivi che verranno eseguiti o installati dopo l'avvio da un supporto SysRescue.

Includi applicazioni esterne: consente di aggiungere programmi esterni alla compilazione SysRescue

Cartella selezionata: cartella in cui si trovano i programmi da aggiungere al disco SysRescue

5.5.2.2 ESET Antivirus

Per la creazione di ESET SysRescue CD, è possibile selezionare due origini di file ESET utilizzabili dal compilatore.

Cartella ESS: file già contenuti nella cartella da cui ESET è stato installato nel computer

File MSI: vengono utilizzati i file contenuti nel programma di installazione di MSI

Profilo: è possibile utilizzare una delle due origini seguite nome utente e password:

ESS installato: il nome utente e la password sono copiati dall'installazione corrente di ESET Smart Security 4 o ESET NOD32

Dall'utente: vengono utilizzati il nome utente e la password immessi nelle caselle di testo corrispondenti

Nota: *ESET Smart Security 4 e ESET NOD32 Antivirus disponibili in ESET SysRescue CD vengono aggiornati via Internet o mediante la soluzione ESET Security installata nel computer in cui è eseguito ESET SysRescue CD.*

5.5.2.3 Avanzate

La scheda **Avanzate** consente di ottimizzare ESET SysRescue CD rispetto alle dimensioni della memoria del computer. Selezionare **512 MB o più** per scrivere il contenuto del CD nella memoria operativa (RAM). Se si seleziona **meno di 512 MB**, durante l'esecuzione di WinPE sarà sempre possibile accedere al CD di ripristino.

Driver esterni. In questa sezione è possibile immettere i driver per gli hardware specifici utilizzati dall'utente (in genere, la scheda di rete). Sebbene WinPE sia basato su Windows Vista SP1, che supporta una vasta gamma di hardware, talvolta l'hardware non viene riconosciuto ed è necessario aggiungere il driver manualmente. Esistono due modi per introdurre il driver nella compilazione di ESET SysRescue : manualmente (mediante il pulsante **Aggiungi**) e automaticamente (mediante il pulsante **Ricerca aut.**). In caso di introduzione manuale, è necessario selezionare il percorso del file .inf corrispondente (occorre inoltre inserire in questa cartella anche il file *.sys applicabile). In caso di introduzione automatica, il driver viene rilevato automaticamente nel sistema operativo di un dato computer. Si consiglia di utilizzare l'introduzione automatica unicamente se SysRescue viene utilizzato su un computer che dispone della stessa scheda di rete utilizzata dal computer in cui è stato creato SysRescue. Durante la creazione di ESET SysRescue il driver viene introdotto nella compilazione in modo tale che l'utente non debba cercarlo in seguito.

5.5.2.4 Supporto USB di avvio

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile selezionare uno dei supporti USB disponibili nella scheda Supporto USB di avvio (nel caso siano presenti più dispositivi USB).

Avvertenza: *Durante il processo di creazione di ESET SysRescue il dispositivo USB selezionato verrà formattato, in altre parole tutti i dati contenuti nel dispositivo verranno eliminati.*

5.5.2.5 Masterizzazione

Se il supporto di destinazione selezionato è CD/DVD, è possibile specificare parametri aggiuntivi di masterizzazione nella scheda Masterizza.

Elimina file ISO: selezionare questa opzione per eliminare i file ISO dopo la creazione del CD di ripristino di ESET.

Eliminazione attivata: consente di selezionare le opzioni per l’eliminazione rapida e completa.

Dispositivo di masterizzazione: selezionare il file da utilizzare per la masterizzazione.

Avvertenza: *Questa è l’opzione predefinita. Se viene utilizzato un CD/DVD riscrivibile, tutti i dati in esso contenuti verranno eliminati.*

La sezione Supporto contiene le informazioni sul supporto correntemente inserito nel dispositivo CD/DVD in uso.

Velocità di masterizzazione: selezionare la velocità desiderata dal menu a discesa. È necessario tenere in considerazione le capacità del dispositivo di masterizzazione e il tipo di CD/DVD utilizzati quando si seleziona la velocità di masterizzazione.

5.5.3 Utilizzo di ESET SysRescue

Affinché il CD/DVD/USB di ripristino funzioni in maniera ottimale, è necessario avviare il computer dal supporto ESET SysRescue. È possibile modificare la priorità di avvio nel BIOS. In alternativa, è possibile attivare il menu di avvio durante l’inizializzazione del computer; in genere si utilizzano i tasti F9 o F12 a seconda della versione della scheda madre/BIOS in uso.

Dopo l’avvio, ESS/ENA viene inizializzato. Poiché ESET SysRescue viene utilizzato solo in situazioni specifiche, l’utilizzo di alcuni moduli di protezione e funzioni del programma disponibili nella versione base di ESS/ENA non è richiesto; l’elenco di tali funzioni e moduli si limita alle operazioni di controllo del computer, aggiornamento e ad alcune sezioni di Imposta. La funzionalità più importante di ESET SysRescue consiste nella capacità di aggiornamento del database delle firme antivirali. Si consiglia di aggiornare il programma prima di avviare il controllo del computer.

5.5.3.1 Utilizzo di ESET SysRescue

Si supponga che i computer nella rete siano stati infettati da un virus che modifica i file eseguibili (EXE). ESS/ENA è in grado eseguire la pulitura di tutti i file infetti ad eccezione di explorer.exe, che non può essere pulito neanche in modalità sicura.

Questo è dovuto al fatto che explorer.exe, in quanto processo essenziale di Windows, viene avviato proprio in modalità sicura. ESS/ENA non può eseguire alcuna azione su questo file che, pertanto, rimane infetto.

In uno scenario simile, per risolvere il problema è possibile ricorrere a ESET SysRescue. ESET SysRescue non richiede l’utilizzo di nessun componente del sistema operativo che lo ospita. Per questo motivo è capace di elaborare (eseguire la pulitura, eliminare) tutti i file sul disco.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili e i documenti. Per replicarsi, un virus allega se stesso all'interno di un file ospite. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base a diversi livelli di attività e di gravità. Alcuni di essi sono estremamente dannosi poiché dispongono della capacità di eliminare di proposito i file da un disco rigido. Altri, invece, non causano veri e propri danni, il loro scopo è quello di infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

È importante tenere presente che i virus (se paragonati a trojan e spyware) stanno diventando una rarità, poiché non sono commercialmente convenienti per gli autori di software dannoso. Inoltre, il termine "virus" è spesso utilizzato in modo scorretto per indicare tutti i tipi di infiltrazioni. Attualmente, questo termine è stato superato dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare i file infetti al loro stato originale, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer ospiti e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente. Non dipendono dai file degli ospiti o dai settori di avvio.

I worm proliferano per mezzo di pacchetti di e-mail o di rete. Pertanto, i worm possono essere classificati in due categorie:

- **Email:** si distribuiscono autonomamente agli indirizzi email dell'elenco dei contatti dell'utente
- **Rete:** sfruttano le vulnerabilità di diverse applicazioni.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore dal rilascio e, in alcuni casi, perfino entro pochi minuti. Questa capacità di replicarsi indipendentemente e rapidamente li rende molto più pericolosi rispetto ad altri tipi di malware, ad esempio i virus.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare alcuni programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

Tra i worm più noti-si segnalano: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Cavalli di Troia

Storicamente, i cavalli di Troia sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Tuttavia, è importante notare che ciò era vero per i cavalli di Troia del passato perché oggi tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "cavallo di Troia" ha assunto un'accezione molto generale che indica un'infiltrazione che non ricade in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie. Le più conosciute sono:

- downloader: un programma dannoso in grado di scaricare altre infiltrazioni da Internet.
- dropper: un tipo di cavallo di troia concepito per installare sui computer compromessi altri tipi di programmi dannosi.
- backdoor: un'applicazione che comunica con gli aggressori remoti, consentendo loro di ottenere l'accesso a un sistema e prenderne il controllo.
- keylogger (registratore delle battute dei tasti): un programma che registra ogni informazione digitata dall'utente e che invia l'informazione agli aggressori remoti.
- dialer: i dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre più di rado.

Solitamente, i cavalli di Troia assumono la forma di file eseguibili con estensione .exe. Se sul computer in uso viene rilevato un file classificato come cavallo di Troia, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

Tra i cavalli di Troia più-noti si segnalano: NetBus, Trojandownloader.Small.ZL, Slapper

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono ad utenti malintenzionati di Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per evitare il rilevamento da parte del software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per questa ragione, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di test.

Per la prevenzione dei rootkit, occorre tenere presente che esistono due livelli di rilevamento:

1. Quando tentano di accedere a un sistema. Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti ai normali test. Il sistema antivirus ESET dispone della tecnologia Anti stealth in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra pop-up con della pubblicità all'interno di un browser oppure modificano la

pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono agli sviluppatori di coprire i costi di sviluppo delle proprie applicazioni (in genere utili).

L'adware di per sé non è pericoloso, ma gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere funzioni di rilevamento e registrazione, allo stesso modo dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware. Tuttavia, in alcuni casi i programmi non vengono installati senza adware oppure le funzioni del programma risultano limitate. Ne consegue che l'adware può spesso accedere al sistema in modo "legale", perché l'utente ha in realtà acconsentito. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa.

Se sul computer in uso viene rilevato un file classificato come adware, è consigliabile eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Si avvalgono di funzioni di controllo per inviare dati statistici di vario tipo, ad esempio l'elenco dei siti Web visitati, gli indirizzi email della rubrica dell'utente o l'elenco dei tasti digitati.

Gli autori di spyware affermano che queste tecniche hanno l'obiettivo di raccogliere informazioni sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware spesso sono accoppiati a versioni gratuite di un programma dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento non contenente tale programma.

Esempi di prodotti freeware noti-che contengono programmi spyware sono le applicazioni client delle reti P2P (peer-to-peer). Spyfalcon o Spy Sheriff (e altri ancora) appartengono a una sottocategoria di spyware specifica – si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se sul computer in uso viene rilevato un file classificato come spyware, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.7 Applicazioni potenzialmente pericolose

Esistono molti programmi legali che servono a semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. Ecco perché ESET ha creato questa particolare categoria. I nostri clienti hanno la possibilità di scegliere se il sistema antivirus deve rilevare tali minacce o meno.

"Applicazioni potenzialmente pericolose" è la classificazione utilizzata per il software sicuro e commerciale. Questa classificazione include programmi quali gli strumenti di accesso remoto, applicazioni di password-cracking e applicazioni di keylogging (programmi che registrano ogni informazione digitata da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

6.1.8 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose, tuttavia potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- apertura di nuove finestre mai viste in precedenza
- attivazione ed esecuzione di processi nascosti
- utilizzo maggiore delle risorse del sistema
- modifiche nei risultati di ricerca
- applicazioni che comunicano con server remoti

6.2 Tipi di attacchi remoti

Esistono molte tecniche particolari che consentono ad utenti remoti di compromettere i sistemi remoti. Tali tecniche sono suddivise in diverse categorie.

6.2.1 Attacchi DoS (Denial of Service)

DoS, acronimo di Denial of Service ovvero negazione del servizio, è un attacco con cui si tenta di rendere il computer o la rete non disponibile per gli utenti. Le comunicazioni fra utenti con problemi simili vengono bloccate e non possono più continuare in modo funzionale. I computer esposti ad attacchi DoS devono essere, in genere, riavviati.

Nella maggior parte dei casi, i bersagli preferiti per questo tipo di attacchi sono i server Web e lo scopo è renderli non disponibili agli utenti per un determinato periodo di tempo.

6.2.2 Poisoning DNS

Attraverso il metodo di poisoning del DNS (Domain Name Server), gli hacker possono ingannare il server DNS di qualsiasi computer facendo credere che i dati fasulli forniti siano invece legittimi e autentici. Queste informazioni fasulle vengono quindi memorizzate nella cache per un determinato periodo di tempo, consentendo agli utenti malintenzionati di riscrivere le risposte DNS per gli indirizzi IP. Di conseguenza, gli utenti che tentano di accedere a siti Web su Internet scaricheranno nel computer virus o worm, invece dei contenuti originali.

6.2.3 Attacchi worm

Un worm è un programma contenente codice dannoso che attacca i computer ospiti e si diffonde tramite una rete. I worm di rete sfruttano le vulnerabilità di diverse applicazioni. Grazie alla disponibilità di Internet, possono diffondersi in tutto il mondo entro poche ore dal loro rilascio, e, in alcuni casi, perfino entro pochi minuti.

La maggior parte degli attacchi worm (Sasser, SqlSlammer) possono essere evitati utilizzando le impostazioni di protezione predefinite del firewall, oppure bloccando le porte non protette e inutilizzate. Inoltre, è essenziale installare le patch di sicurezza più recenti per il sistema operativo in uso.

6.2.4 Scansione porte

La scansione porta controlla se sono presenti porte del computer aperte su un host di rete. Uno scanner di porte è un software progettato per rilevare tali porte.

La porta di un computer è un punto virtuale che gestisce i dati in entrata e in uscita: un elemento strategico dal punto di vista della sicurezza. In una rete di grandi dimensioni, le informazioni raccolte dagli scanner di porta possono contribuire a identificare le potenziali vulnerabilità. Tale uso è legittimo.

Tuttavia, la scansione delle porte viene spesso utilizzata dagli hacker nel tentativo di compromettere la sicurezza. Per prima cosa, gli hacker inviano pacchetti a ogni porta. A seconda del tipo di risposta, è possibile stabilire quali sono le porte in uso. La scansione in sé non causa danni, ma occorre tenere presente che questa attività può rivelare le potenziali vulnerabilità e consente ad utenti malintenzionati di prendere il controllo dei computer remoti.

Si consiglia agli amministratori di rete di bloccare tutte le porte inutilizzate e proteggere quelle in uso dagli accessi non autorizzati.

6.2.5 Desincronizzazione TCP

La desincronizzazione TCP è una tecnica utilizzata negli attacchi Hijacking TCP. È avviata da un processo in cui il numero sequenziale dei pacchetti in entrata è diverso dal numero sequenziale atteso. I pacchetti con un numero sequenziale inatteso vengono ignorati (o salvati nel buffer, se sono presenti nella finestra della comunicazione corrente).

In stato di desincronizzazione, entrambi gli endpoint della comunicazione ignorano i pacchetti ricevuti. Questo è il momento in cui gli utenti malintenzionati remoti sono in grado di infiltrarsi e fornire pacchetti con un numero di sequenza corretto. Gli aggressori sono persino in grado di manipolare la comunicazione tramite i loro comandi, oppure modificarla in qualche modo.

Gli attacchi Hijacking mirano all'interruzione delle comunicazioni server-client o peer-to-peer. Molti attacchi possono essere evitati utilizzando l'autenticazione per ciascun segmento TCP. È inoltre opportuno utilizzare le configurazioni consigliate per i dispositivi di rete in uso.

6.2.6 SMB Relay

SMBRelay e SMBRelay2 sono programmi in grado di infliggere un attacco ai computer remoti. Questi programmi si avvalgono del protocollo di condivisione file SMB (Server Message Block) sovrapposto su NetBIOS. Se un utente condivide una cartella o una directory all'interno della LAN, con tutta probabilità utilizza questo protocollo di condivisione file.

Nell'ambito della comunicazione della rete locale, vengono scambiate password hash.

SMBRelay riceve una connessione sulle porte UDP 139 e 445, inoltra i pacchetti scambiati dal client e dal server e li modifica. Dopo aver eseguito la connessione e l'autenticazione, il client viene disconnesso. SMBRelay crea un nuovo indirizzo IP virtuale. È possibile accedere al nuovo indirizzo utilizzando il comando "net use \\192.168.1.1". L'indirizzo può quindi essere utilizzato da qualsiasi funzione di rete di Windows. SMBRelay inoltra la comunicazione del protocollo SMB tranne che per la negoziazione e l'autenticazione. Gli utenti malintenzionati remoti possono utilizzare l'indirizzo IP purché il computer client sia connesso.

SMBRelay2 funziona in base agli stessi principi di SMBRelay, solo che utilizza i nomi NetBIOS invece degli indirizzi IP. Entrambi sono in grado di infliggere attacchi di tipo MITM (man-in-the-middle). Questi attacchi consentono agli utenti malintenzionati remoti di leggere, inserire e modificare i messaggi scambiati tra due endpoint di comunicazione senza essere notati. I computer esposti a tali attacchi spesso non rispondono più o si riavviano inaspettatamente.

Per evitare gli attacchi, si consiglia di utilizzare password o chiavi di autenticazione.

6.2.7 Attacchi ICMP

ICMP (Internet Control Message Protocol) è un protocollo Internet molto diffuso e ampiamente utilizzato. Viene usato principalmente dai computer in rete per inviare diversi messaggi di errore.

Gli utenti malintenzionati in remoto tentano di sfruttare i punti deboli del protocollo ICMP. Il protocollo ICMP è stato progettato per la comunicazione uni-direzionale che non prevede l'autenticazione. Questo consente agli utenti malintenzionati di sferrare i cosiddetti attacchi DoS (Denial of Service) o attacchi che consentono a utenti non autorizzati di accedere ai pacchetti in ingresso e in uscita.

Esempi tipici di attacchi ICMP includono attacchi ping flood, ICMP_ECHO flood e smurf. I computer esposti ad attacchi ICMP risultano notevolmente più lenti (ciò è relativo a tutte le applicazioni che utilizzano Internet) e presentano problemi di connessione a Internet.

6.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È un servizio flessibile, rapido e diretto. I messaggi e-mail hanno svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa del loro elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Tra gli esempi tipici di messaggi di spam figurano annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli per gli utenti è il fatto che i costi di invio dei messaggi sono minimi e gli autori di messaggi di spam dispongono di numerosi strumenti e risorse per acquisire nuovi indirizzi e-mail. Inoltre, il volume e la varietà dei messaggi di spam ne rende estremamente difficoltoso il controllo. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spam. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo email su Internet
- Fornire il proprio indirizzo email solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a caselle di controllo di tipo "Sì, desidero ricevere informazioni su... nella posta in arrivo".
- Utilizzare indirizzi email "specializzati", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via
- Cambiare di tanto in tanto l'indirizzo email
- Utilizzare una soluzione antispam

6.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. Per la pubblicità tramite e-mail si utilizzano i messaggi e-mail come strumento di contatto. I vantaggi principali dal punto di vista del marketing sono i costi zero e un livello elevato di immediatezza ed efficacia; inoltre, i messaggi vengono recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo strumento pubblicitario è legittimo, perché un utente può essere interessato a ricevere informazioni commerciali su determinati prodotti. Ma il problema è che molte società inviano messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi email commerciali non desiderati diventa così un problema concreto, poiché non mostra segni di flessione. Gli autori di messaggi e-mail non desiderati tentano ovviamente di mascherare i messaggi di spam come messaggi legittimi. D'altra parte, la pubblicità

legittima in grandi quantità può provocare reazioni negative.

6.3.2 Hoax: truffe e bufale

Un hoax è un messaggio diffuso su Internet che viene in genere inviato via e-mail e talvolta tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax hanno solo lo scopo di diffondere il panico. Ai destinatari viene in genere chiesto di inoltrare il messaggio a tutti i relativi contatti, perpetuando il ciclo-di vita dell'hoax. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Nella maggior parte dei casi è impossibile tenere comprendere le intenzioni dell'autore del messaggio.

Occorre tener presente che generalmente i messaggi che invitano ad essere inoltrati a tutti i propri conoscenti potrebbero essere hoax. Su Internet sono presenti molti siti Web specializzati in grado di verificare l'autenticità di un messaggio email. Prima di eseguire l'inoltro, effettuare una ricerca in Internet per qualsiasi messaggio sospetto se si ritiene si tratti di hoax.

6.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che potrebbero essere utilizzati dalla fonte originaria che viene usata dal messaggio stesso. Con tali messaggi si chiede all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di inviare alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo fraudolento.

Ricordare sempre che le banche, le compagnie di assicurazioni e altre società legittime non chiedono mai di rivelare nomi utente e password in messaggi email non richiesti.

6.3.4 Riconoscimento di messaggi spam

Esistono, generalmente, alcuni indicatori che consentono di identificare i messaggi spam (e-mail non desiderate) nella casella di posta. Un messaggio può essere considerato un messaggio spam se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino tuttavia ad anticipare una piccola somma di denaro
- Viene chiesto di immettere con vari pretesti (verifica di dati, operazioni finanziarie) alcuni dati personali, quali numero di conto bancario, nome utente, password e così via
- È scritto in una lingua straniera
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un fornitore attendibile (contattare il produttore originale)
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro di spam, ad esempio "vaigra" invece di "viagra" e così via

6.3.4.1 Regole

Nell'ambito delle soluzioni antispam e dei client di posta, le regole sono strumenti per manipolare le funzioni della posta elettronica. Sono composte da due parti logiche:

1. condizione (ad esempio, un messaggio in arrivo da un determinato indirizzo)

2. azione (ad esempio, eliminazione del messaggio, spostamento in una cartella specificata).

Il numero e la combinazione di regole varia a seconda della soluzione antispam. Queste regole rappresentano delle misure contro i messaggi di spam (e-mail indesiderate). Esempi tipici:

- 1. condizione: un messaggio in arrivo contiene alcune delle parole generalmente inserite nei messaggi di spam
  2. azione: eliminare il messaggio
- 1. condizione: un messaggio email in arrivo contiene un allegato con estensione .exe
  2. azione: eliminare l'allegato e recapitare il messaggio alla casella di posta
- 1. condizione: un messaggio in arrivo inviato dal datore di lavoro dell'utente
  2. azione: spostare il messaggio nella cartella "Lavoro".

È consigliabile utilizzare una combinazione di regole nei programmi antispam per semplificare l'amministrazione e filtrare più efficacemente i messaggi di spam (email indesiderate).

6.3.4.2 Filtro Bayes

Il filtro di spam Bayes è un tipo di filtro email molto efficace, utilizzato da quasi tutti i prodotti antispam. È in grado di identificare messaggi e-mail non desiderati con un alto livello di precisione e può essere personalizzato.

La funzionalità si basa sul principio seguente: il processo di conoscenza avviene nella prima fase. L'utente contrassegna manualmente un numero sufficiente di messaggi come legittimi o come spam (in genere 200/200). Il filtro analizza entrambe le categorie e apprende, ad esempio, che i messaggi spam contengono in genere parole come "rolex" o "viagra", mentre i messaggi legittimi sono inviati da familiari o da indirizzi presenti nell'elenco contatti dell'utente. Con un numero sufficiente di messaggi elaborati, il filtro Bayes è in grado di assegnare un determinato "indice di spam" a ciascun messaggio e determinare se si tratta o meno di spam.

Il vantaggio principale è la flessibilità del metodo. Se, ad esempio, un utente è un biologo, verrà assegnato un indice di probabilità basso a tutti i messaggi email in arrivo che riguardano la biologia o relativi campi di studio. Se un messaggio comprende parole che potrebbero identificarlo come non richiesto, ma proviene da un utente presente in un elenco di contatti, verrà contrassegnato come legittimo, perché per i mittenti contenuti in un elenco di contatti diminuisce la probabilità generale di spam.

6.3.4.3 Whitelist

In generale, una whitelist è un elenco di voci o di persone accettate a cui è stata concessa l'autorizzazione di accesso. Il termine "whitelist di posta" definisce un elenco di contatti da cui l'utente desidera ricevere messaggi. Tali whitelist sono basate su parole chiave ricercate negli indirizzi e-mail, nei nomi di domini o negli indirizzi IP.

Se una whitelist funziona in "modalità di esclusività", i messaggi che provengono da qualsiasi altro indirizzo, dominio o indirizzo IP non verranno ricevuti. Se non è esclusiva, tali messaggi non verranno

eliminati ma solo filtrati in qualche altro modo.

Una whitelist si basa sul principio opposto di quello di una blacklist. Le whitelist sono relativamente facili da mantenere, molto di più rispetto alle blacklist. Si consiglia di utilizzare sia la whitelist che la blacklist per filtrare più efficacemente i messaggi di spam.

6.3.4.4 Blacklist

In genere, una blacklist è un elenco di persone o elementi non accettati o vietati. Nel mondo virtuale, è una tecnica che consente di accettare messaggi provenienti da tutti gli utenti non presenti in questo elenco.

Esistono due tipi di blacklist ed è possibile creare blacklist personalizzate tramite il programma antispam in uso. D'altra parte, su Internet è possibile trovare molte blacklist di tipo professionale, aggiornate regolarmente e create da istituzioni specializzate.

Una blacklist si basa sul principio contrario a quello di una whitelist. Le blacklist sono un elemento essenziale per bloccare i messaggi di spam, ma sono difficili da gestire perché ogni giorno si presentano nuovi elementi da bloccare. È quindi consigliabile utilizzare sia whitelist che blacklist per filtrare i messaggi di spam in modo più efficace.

6.3.4.5 Controllo lato server

Il controllo lato server è una tecnica che consente di identificare e-mail spam di massa in base al numero di messaggi ricevuti e alle reazioni degli utenti. Ciascun messaggio lascia una "impronta" digitale univoca sul server in base al contenuto. In realtà, si tratta di un numero ID univoco che non fornisce molte informazioni sul contenuto del messaggio e-mail. Due messaggi identici avranno impronte identiche, mentre messaggi diversi avranno impronte diverse.

Se un messaggio viene contrassegnato come spam, l'impronta corrispondente viene inviata al server. Se il server riceve più impronte identiche (che corrispondono a un determinato messaggio di spam), l'impronta viene memorizzata nel database di impronte di spam. Durante il controllo dei messaggi in arrivo, il programma invia le impronte dei messaggi al server. Il server restituisce informazioni sulle impronte corrispondenti ai messaggi già contrassegnati dagli utenti come spam.